ESET NOD32 Antivírus 3.0

Componentes integrados:
ESET NOD32 Antivírus
ESET NOD32 Antispyware

Guia do usuário

eset nós protegemos seu universo digital

conteúdo

ESET NOD32 Antivírus 3.0

Atendimento ao cliente mundial: www.eset.eu/support
Atendimento ao cliente da América do Norte: www.eset.com/support

REV.20080509-001

1. ESET NOD32 Antivírus 3.0

O ESET NOD32 Antivírus 3.0 é o sucessor do premiado produto ESET NOD32 Antivírus 2.*. Ele utiliza a velocidade de rastreamento e a precisão do ESET NOD32 Antivírus, garantida pela versão mais recente do mecanismo de busca ThreatSense®.

As técnicas avançadas implementadas são capazes de bloquear, de maneira proativa, vírus, spyware, cavalos de tróia, worms, adware e rootkits sem reduzir a velocidade do sistema ou perturbá-lo enquanto você trabalha ou joga no computador.

1.1 O que há de novo

A experiência em desenvolvimento de longo prazo de nossos especialistas é demonstrada por toda a nova arquitetura do programa ESET NOD32 Antivírus, que garante máxima detecção com o mínimo de exigências do sistema.

- **Antivírus e antispyware**

Esse módulo é construído sobre a unidade central de rastreamento ThreatSense®, que foi usada pela primeira vez no premiado sistema NOD 32 Antivírus. A unidade central ThreatSense® é otimizada e melhorada com a nova arquitetura do ESET NOD32 Antivírus.

Recurso	Descrição
Limpeza melhorada	O sistema antivírus agora limpa e exclui inteligentemente a maioria das infiltrações detectadas, sem exigir a intervenção do usuário.
Modo de Rastreamento em Segundo Plano	O rastreamento do computador pode ser iniciado em segundo plano sem diminuir o desempenho.
Arquivos de Atualização Menores	O processo de otimização central mantém o tamanho dos arquivos de atualização menores do que na versão 2.7. Também, a proteção dos arquivos de atualização contra danos foi melhorada.
Proteção de Cliente de E-mail Popular	Agora é possível verificar os e-mails recebidos não somente no MS Outlook, mas também no Outlook Express e no Windows Mail.
Diversas Outras Melhorias Menores	– Acesso direto aos sistemas de arquivos para alta velocidade e resultado. – Bloqueio de acesso aos arquivos infectados – Otimização para o Windows Security Center, incluindo o Vista.

1.2 Requisitos do sistema

Para uma operação sem interrupções do ESET NOD32 Antivírus, o sistema deve atender às seguintes exigências de hardware e de software:

ESET NOD32 Antivírus:

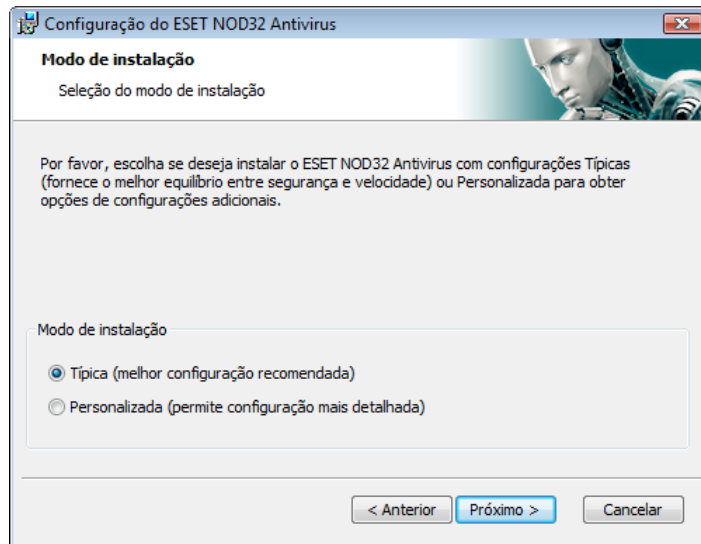
Windows 2000, XP	400 MHz 32 bits / 64 bits (x86 / x64) 128 MB RAM de memória do sistema 35 MB de espaço disponível Super VGA (800 × 600)
Windows Vista	1 GHz 32 bits / 64 bits (x86 / x64) 512 MB RAM de memória do sistema 35 MB de espaço disponível Super VGA (800 × 600)

ESET NOD32 Antivírus Business Edition:

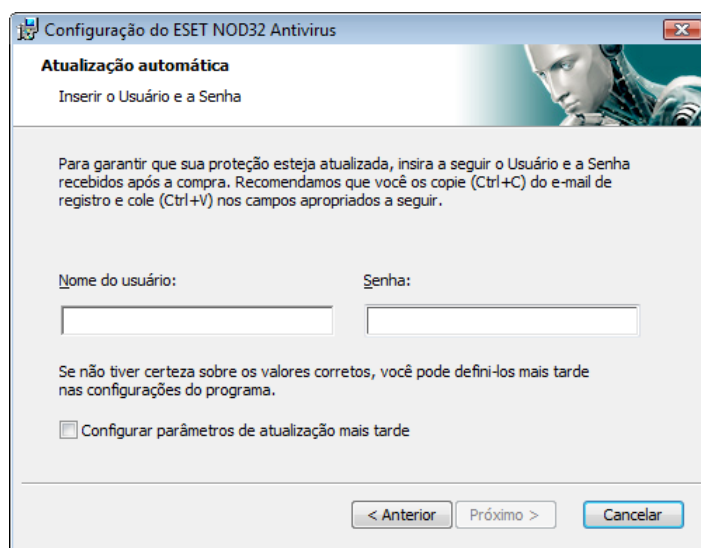
Windows 2000, 2000 Server, XP, 2003 Server	400 MHz 32 bits / 64 bits (x86 / x64) 128 MB RAM de memória do sistema 35 MB de espaço disponível Super VGA (800 × 600)
Windows Vista, Windows Server 2008	1 GHz 32 bits / 64 bits (x86 / x64) 512 MB RAM de memória do sistema 35 MB de espaço disponível Super VGA (800 × 600)

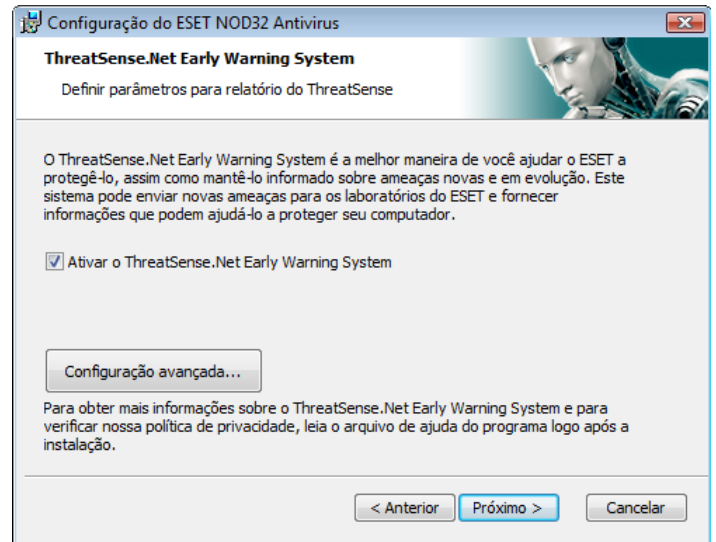
2. Instalação

Após a compra, o instalador do ESET NOD32 Antivírus pode ser obtido através de download no site do ESET na Web como um pacote .msi. Inicie o instalador e o assistente de instalação o guiará pela configuração básica. Há dois tipos de instalação disponíveis com diferentes níveis de detalhes de configuração:

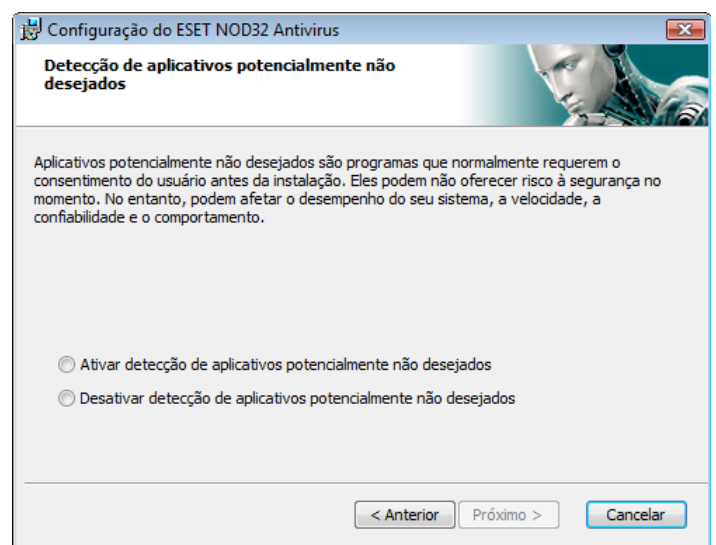
1. Instalação típica
2. Instalação personalizada

2.1. Instalação típica

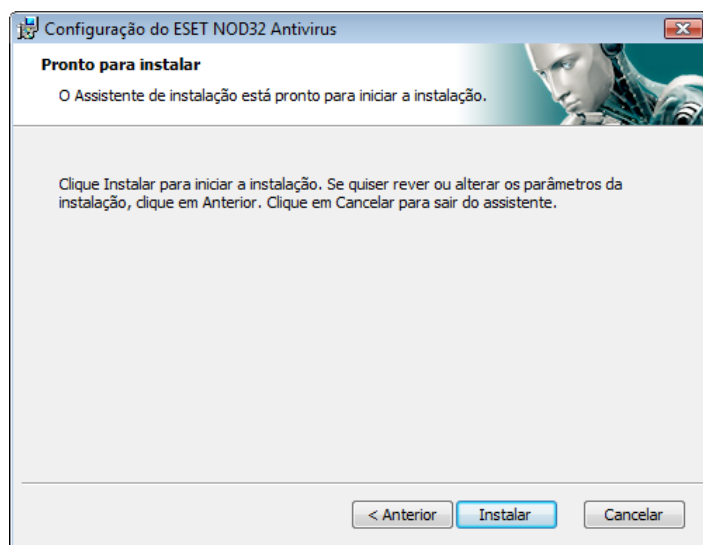
A instalação típica é recomendada para usuários que desejam instalar o ESET NOD32 Antivírus com as configurações padrão. As configurações padrão do programa fornecem o nível máximo de proteção, um fato apreciado pelos usuários que não desejam definir configurações detalhadas.

A primeira e muito importante etapa é inserir o nome de usuário e a senha para a atualização automática do programa. Essa etapa tem um papel significativo no fornecimento de proteção constante ao sistema.

Insira o seu **Nome de usuário** e **Senha**, isto é, os dados de autenticação recebidos após a compra ou registro do produto, nos campos correspondentes. Se você não tiver o Nome de usuário e Senha disponíveis no momento, selecione a opção **Configurar parâmetros de atualização mais tarde**. Os dados de autenticação podem ser inseridos posteriormente a qualquer hora, diretamente no programa.

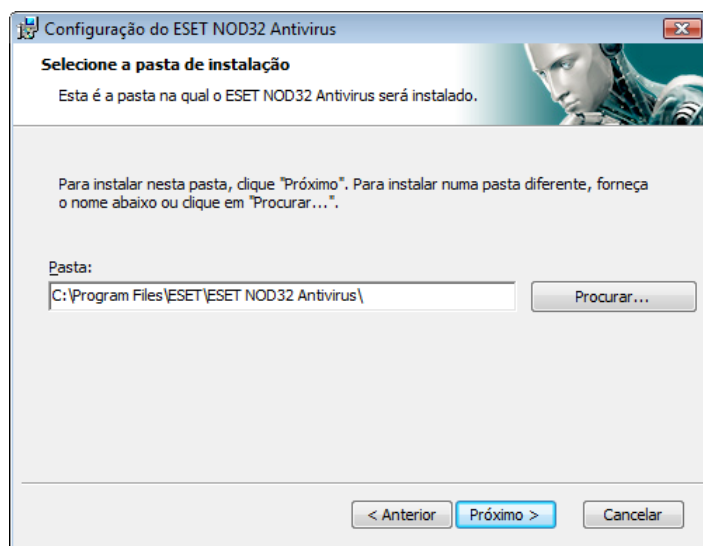
A próxima etapa da instalação é a configuração do ThreatSense.Net Early Warning System. O ThreatSense.Net Early Warning System ajuda a garantir que a ESET seja informada contínua e imediatamente sobre novas ameaças para proteger rapidamente seus clientes. O sistema permite o envio de novas ameaças para o laboratório de vírus da ESET, onde elas são analisadas, processadas e adicionadas à base de dados de assinatura de vírus.

Por padrão, a caixa de seleção **Ativar o ThreatSense.Net Early Warning System** está selecionada, que ativará esse recurso. Clique em **Configuração avançada...** para modificar as configurações detalhadas para o envio de arquivos suspeitos.

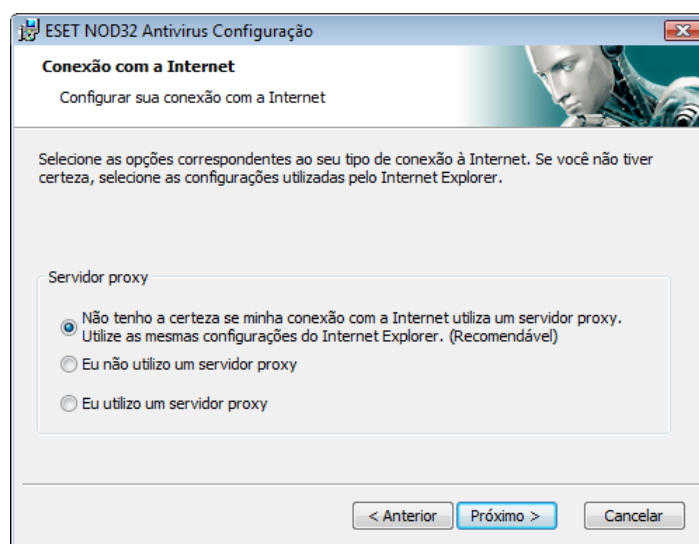
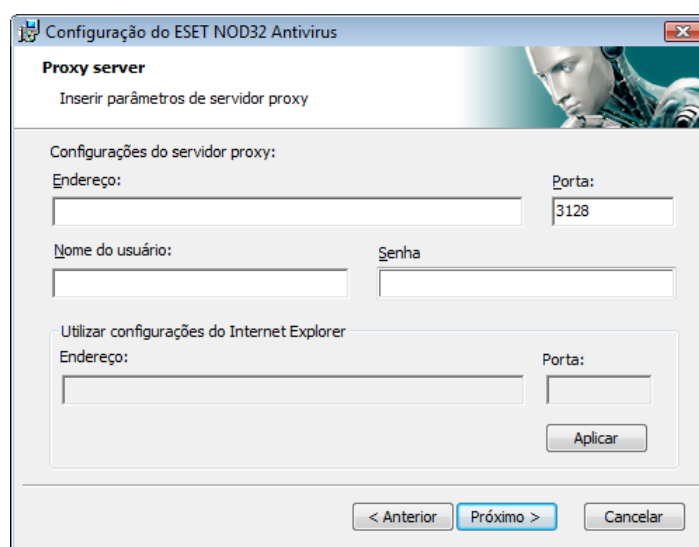
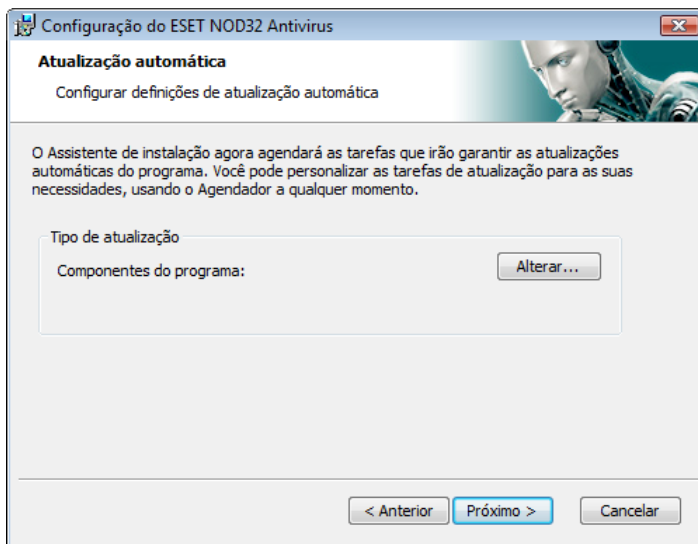
A próxima etapa do processo de instalação é a configuração da **Detecção de aplicativos potencialmente não desejados**. Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar negativamente o comportamento do sistema operacional.

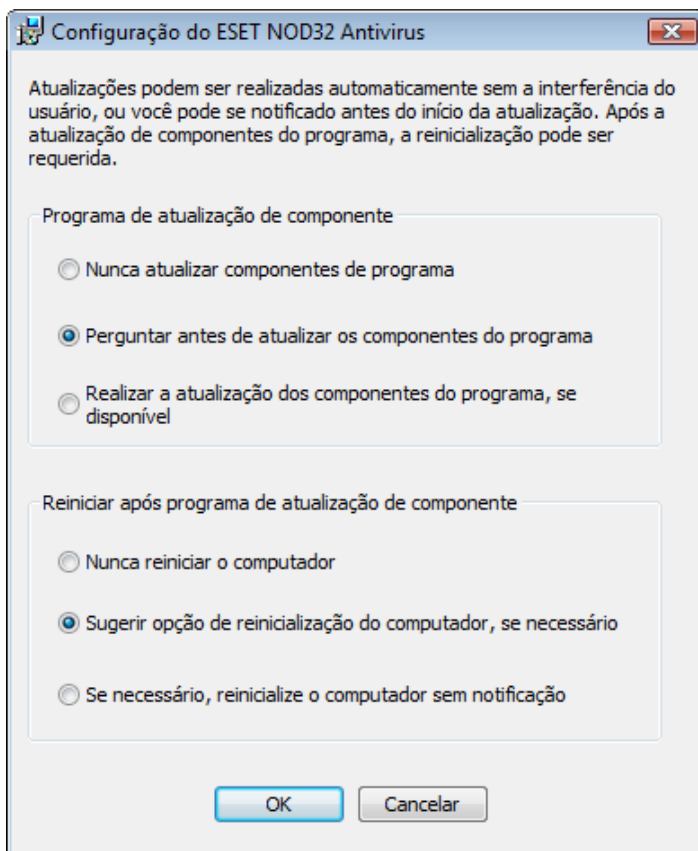
Esses aplicativos são freqüentemente vinculados a outros programas e podem ser difíceis de notar durante o processo de instalação. Embora esses aplicativos geralmente exibam uma notificação durante a instalação, eles podem ser instalados facilmente sem o seu consentimento.

Selecione a opção **Ativar detecção de aplicativos potencialmente não desejados** para permitir que o ESET NOD32 Antivírus detecte este tipo de ameaça (recomendável).

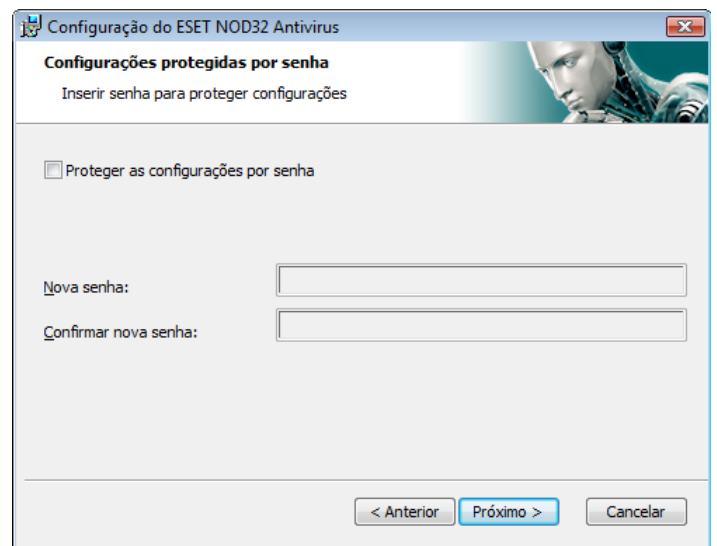
A última etapa no modo de Instalação típica é a confirmação da instalação clicando no botão **Instalar**.

2.2 Instalação personalizada

A **Instalação** personalizada é destinada a usuários experientes em ajuste de programas e que desejam modificar configurações avançadas durante a instalação.

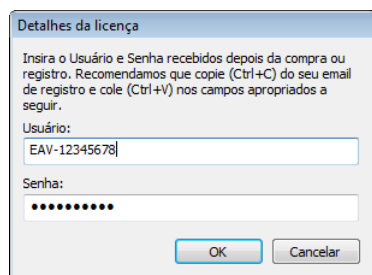
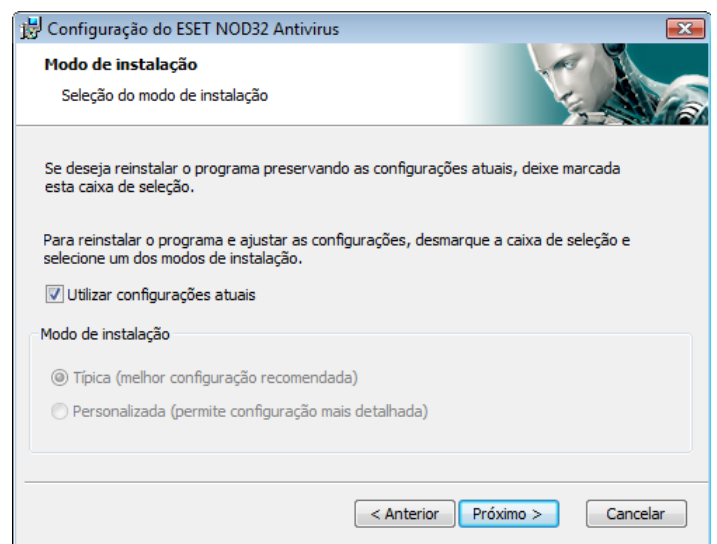
A primeira etapa é selecionar o local de destino para a instalação. Por padrão, o programa é instalado em C:\Arquivos de Programas\ESET\ESET Smart Security\. Clique em **Procurar…** para alterar esse local (não recomendável).

Em seguida, **Inserir nome de usuário e senha**. Essa etapa é igual à da Instalação típica (consulte a página 5).

Após inserir o seu Nome de usuário e Senha, clique em **Avançar** para **Configurar sua conexão com a Internet**.

Se utilizar um servidor proxy, ele deve ser configurado corretamente para que as atualizações de assinatura de vírus funcionem adequadamente. Se não souber se utiliza ou não um servidor proxy para conectar-se à Internet, mantenha a configuração padrão **Não tenho a certeza se a minha conexão com a Internet usa um servidor proxy. Utilize as mesmas configurações do Internet Explorer** e clique em **Avançar**. Se não utilizar um servidor proxy, selecione a opção correspondente.

Para definir as configurações do servidor proxy, selecione **Eu utilizo um servidor proxy** e clique em **Avançar**. Insira o endereço IP ou o URL do seu servidor proxy no campo **Endereço.** No campo **Porta**, especifique a porta em que o servidor proxy aceita as conexões (3128 por padrão). Caso o servidor proxy requeira autenticação, um nome de usuário e senha válidos devem ser inseridos, o que concede acesso ao servidor proxy. As configurações do servidor proxy também podem ser copiadas do Internet Explorer se desejar. Para fazer isso, clique em **Aplicar** e confirme a seleção.

Clique em **Avançar** para prosseguir para a janela **Configurar definições de atualização automática**. Essa etapa permite especificar como as atualizações automáticas dos componentes do programa serão tratadas no sistema. Clique em **Alterar...** para acessar as configurações avançadas.

Se não desejar atualizar os componentes do programa, selecione **Nunca atualizar componentes de programa**. A ativação da opção **Perguntar antes de fazer download dos componentes de programa** exibirá uma janela de confirmação para fazer download dos componentes de programa. Para ativar a atualização automática dos componentes de programa sem avisar, selecione a opção **Realizar a atualização dos componentes do programa, se disponível**.

OBSERVAÇÃO: Após uma atualização dos componentes do programa, uma reinicialização é usualmente necessária. A configuração recomendada é: **Se necessário, reinicialize o computador sem notificação**.

A próxima etapa da instalação é inserir uma senha para proteger os parâmetros do programa. Escolha uma senha com a qual deseja proteger o programa. Digite a senha novamente para confirmar.

As etapas **Configuração do ThreatSense.Net Early Warning System** e **Detecção de aplicativos potencialmente não desejados** são as mesmas de uma Instalação típica e não são mostradas aqui (consulte a página 5).

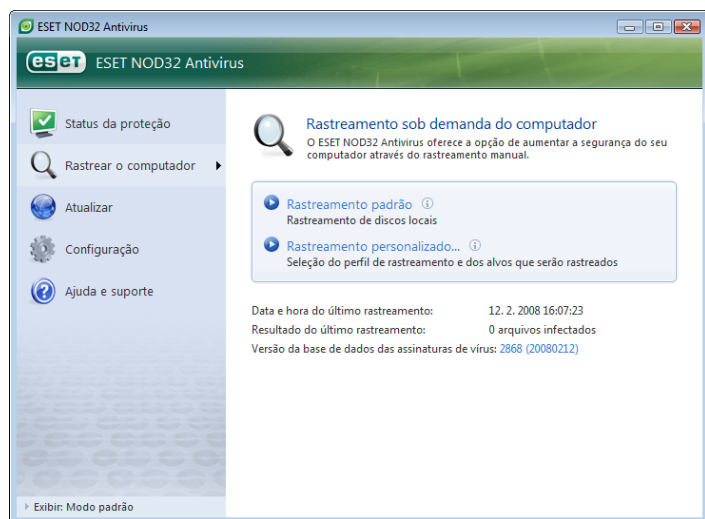
A última etapa mostra uma janela que requer o seu consentimento para instalar.

2.3 Uso de configurações originais

Se você reinstalar o ESET NOD32 Antivírus, a opção **Utilizar configurações atuais** será exibida. Selecione esta opção para transferir os parâmetros de configuração da instalação original para uma nova instalação.

2.4 Inserção do nome de usuário e senha

Para obter a funcionalidade ideal, é importante que o programa seja atualizado automaticamente. Isso somente será possível se o nome de usuário e a senha corretos forem inseridos na configuração da atualização.

Se você não inseriu o seu nome de usuário e senha durante a instalação, você poderá inseri-los agora. Na janela principal do programa, clique na opção **Atualizar** e, em seguida, na opção **Configuração de nome de usuário e senha...** Insira os dados recebidos com a licença do produto na janela **Detalhes da licença**.

2.5 Rastreamento sob demanda do computador

Após a instalação do ESET NOD32 Antivírus, um rastreamento no computador para verificar a presença de código malicioso deverá ser executado. Para iniciar o rastreamento rapidamente, selecione **Rastrear o computador** no menu principal e selecione **Rastreamento padrão** na janela principal do programa. Para obter mais informações sobre o recurso Rastreamento do computador, consulte o capítulo “Rastreamento do computador”.

3. Guia do iniciante

Este capítulo fornece uma visão geral inicial do ESET NOD32 Antivírus e suas configurações básicas.

3.1 Introdução ao design da interface do usuário – modos

A janela principal do ESET NOD32 Antivírus é dividida em duas seções principais. A coluna à esquerda fornece acesso ao menu principal amigável. A janela principal do programa à direita serve principalmente para exibir informações correspondentes à opção selecionada no menu principal.

A seguir há uma descrição dos botões dentro do menu principal:

Status da proteção – De uma forma amigável, ele fornece informações sobre o status de proteção do ESET Smart Security. Se o modo Avançado estiver ativado, o status de todos os módulos de proteção será exibido. Clique em um módulo para exibir o seu status atual.

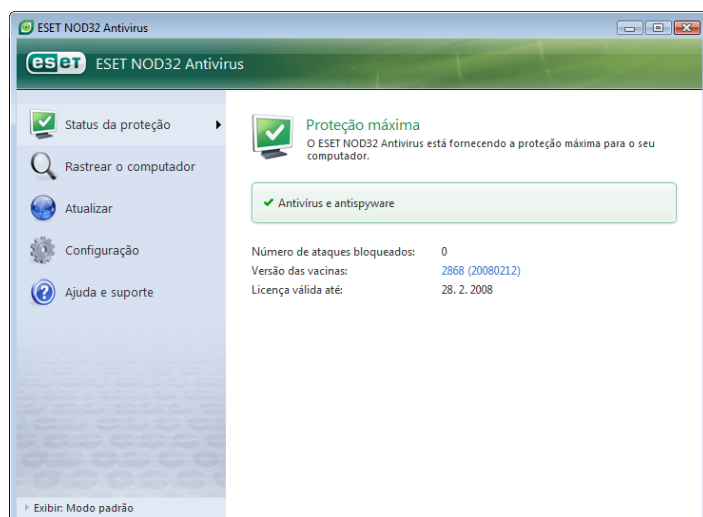
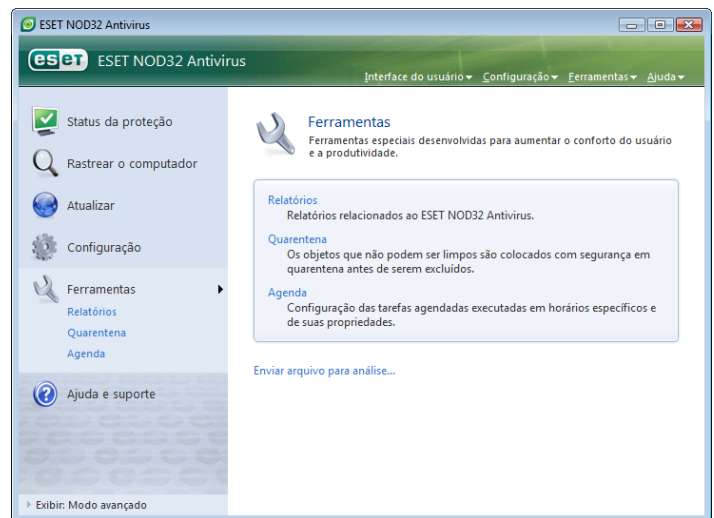
Rastrear o computador – Esta opção permite que o usuário configure e inicie o rastreamento sob demanda do computador.

Atualizar – Selecione esta opção para acessar o módulo de atualização que gerencia as atualizações para a base de dados de assinatura de vírus.

Configuração – Selecione esta opção para ajustar o nível de segurança do seu computador. Se o modo Avançado estiver ativado, o módulo de proteção dos submenus Antivírus and antispyware será exibido.

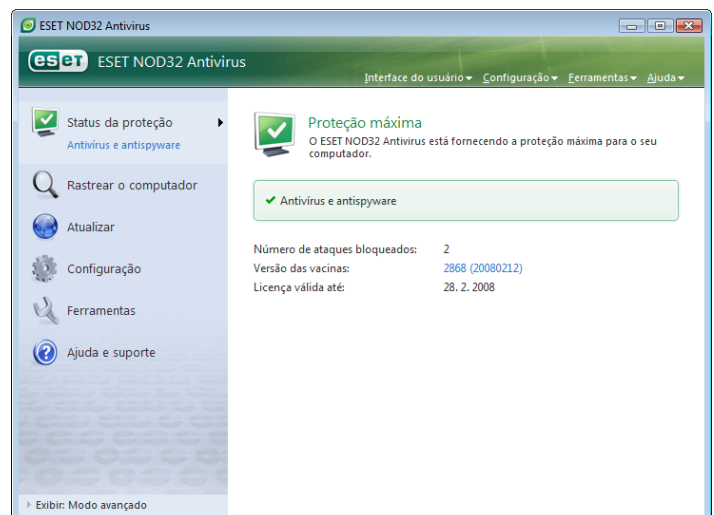
Ferramentas – Esta opção está disponível somente no modo Avançado. Fornece acesso a Relatórios, Quarentena e Agenda.

Ajuda e suporte – Selecione esta opção para acessar os arquivos da ajuda, a base de dados de conhecimento da ESET, o site da ESET na Web e acessar uma solicitação de suporte ao Atendimento ao cliente.

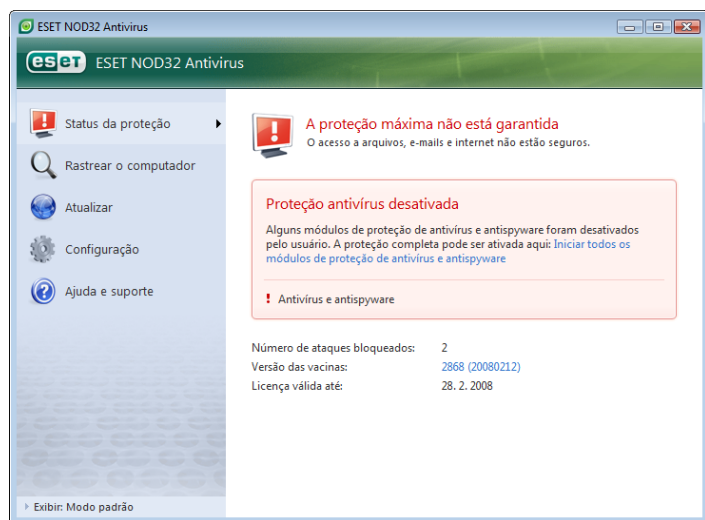
A interface do usuário do ESET NOD32 Antivírus permite que os usuários alternem entre os modos Padrão e Avançado. Para alternar entre os modos, consulte o link **Exibir** localizado no canto inferior esquerdo da tela principal do ESET NOD32 Antivírus. Clique nesse botão para selecionar o modo de exibição desejado.

O modo padrão fornece acesso aos recursos necessários para operações comuns. Ele não exibe opções avançadas.

A alternância para o modo Avançado adiciona a opção **Ferramentas** ao menu principal. A opção Ferramentas permite que o usuário acesse a Agenda, a Quarentena ou exiba os relatórios do ESET NOD32 Antivírus.

OBSERVAÇÃO: Todas as instruções restantes neste guia ocorrerão no modo Avançado.

3.1.1 Verificação do funcionamento do sistema

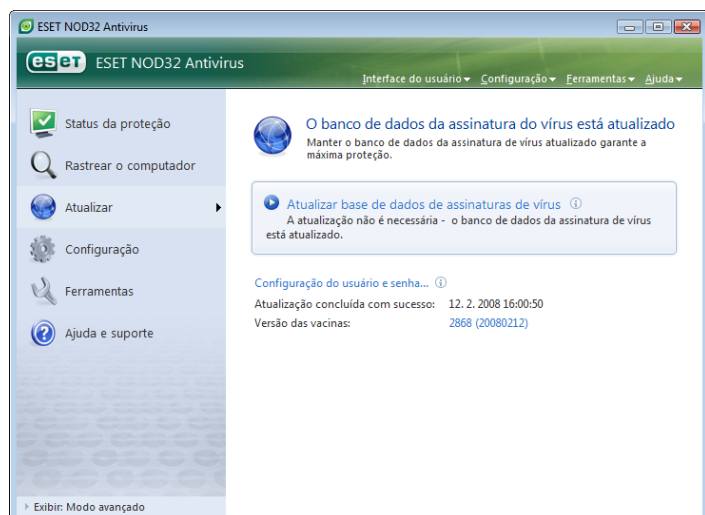
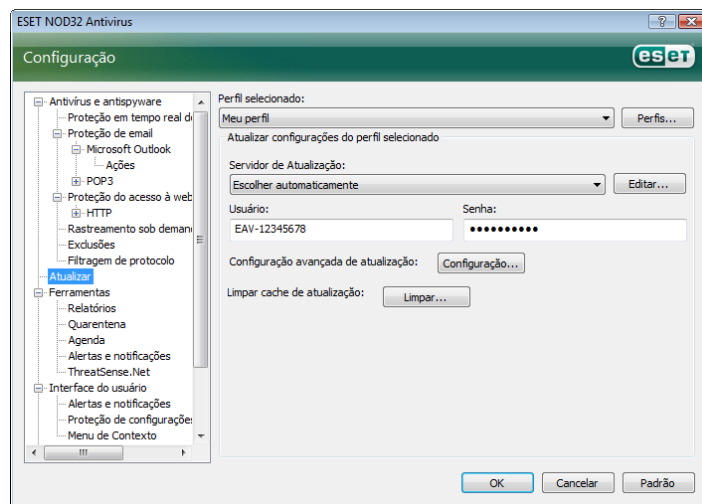
Para exibir o **Status da proteção**, clique nesta opção no topo do menu principal. O submenu **Antivírus e antispyware** será exibido diretamente abaixo, e um resumo de status sobre a operação do ESET NOD32 Antivírus será exibido na janela principal do programa. Após clicar em Antivírus e antispyware, será mostrado na janela principal do programa o status dos módulos de proteção individuais.

Se os módulos ativados estiverem funcionando adequadamente, uma marca verde será atribuída a eles. Caso contrário, um ponto de exclamação vermelho ou um ícone de notificação laranja é exibido, e informações adicionais sobre o módulo serão mostradas na parte superior da janela. Um solução sugerida para corrigir o módulo também é exibida. Para alterar o status dos módulos individuais, clique em **Configuração** no menu principal e clique no módulo desejado.

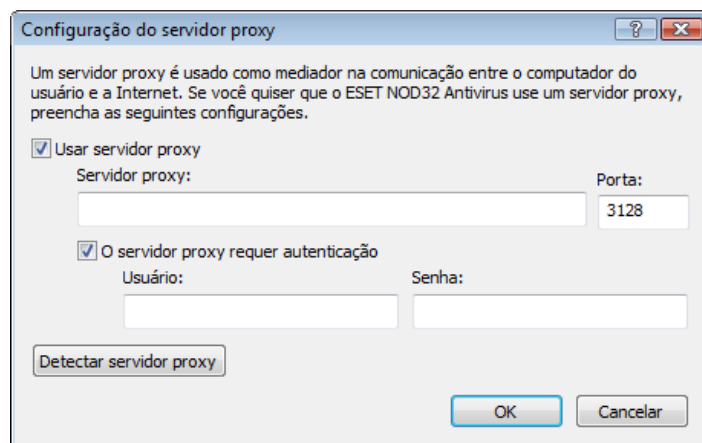
3.1.2 O que fazer se o programa não funciona adequadamente

Se o ESET NOD32 Antivírus detectar um problema em qualquer um dos seus módulos de proteção, ele será relatado na janela **Status da proteção**. Uma sugestão para a solução do problema também é fornecida aqui.

Se não for possível solucionar um problema utilizando a lista exibida de problemas conhecidos e soluções, clique em **Ajuda e suporte** para acessar os arquivos de ajuda ou procurar a Base de dados de conhecimento. Se uma solução ainda não puder ser encontrada, você pode enviar uma solicitação de suporte ao Atendimento ao cliente da ESET. Com base nessas informações fornecidas, nossos especialistas podem responder rapidamente as suas questões e aconselhá-lo com mais eficiência sobre o problema.

3.2 Configuração da atualização

A atualização da base de dados da assinatura de vírus e a atualização dos componentes do programa são partes importantes no fornecimento de proteção completa contra códigos maliciosos. Dê atenção especial à configuração e operação delas. No menu principal, selecione **Atualizar** e clique em **Atualizar base de dados de assinatura de vírus** na janela principal do programa para verificar instantaneamente quanto à disponibilidade de uma atualização de base de dados mais nova. **Configuração de nome de usuário e senha...** exibe uma caixa de diálogo em que o Nome de usuário e Senha recebidos no momento da compra devem ser inseridos.

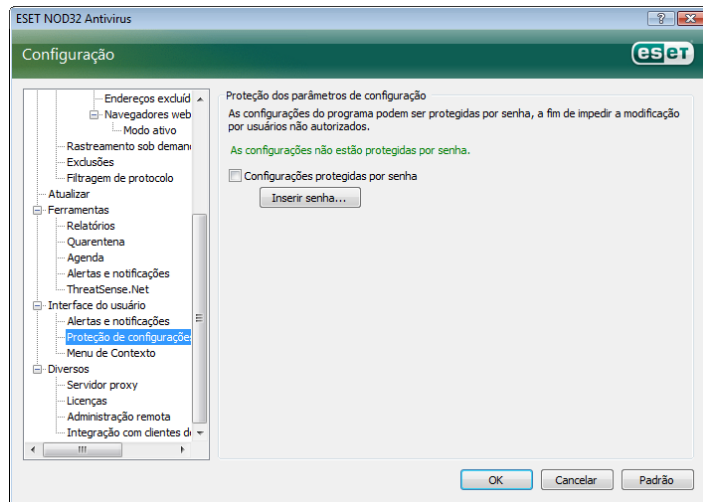
Se o Nome de usuário e a Senha foram inseridos durante a instalação do ESET NOD32 Antivírus, você não será solicitado a fornecê-los neste ponto.

A janela **Configuração avançada** (pressione F5 para acessar) contém outras opções de atualização detalhadas. O menu suspenso **Atualizar servidor:** deve ser configurado como **Escolher automaticamente**. Para configurar as opções de atualização avançadas, como o modo de atualização, o acesso ao servidor proxy, acessando as atualizações em um servidor local e criando cópias de assinatura de vírus (ESET NOD32 Antivírus Business Edition), clique no botão **Configuração...**

3.3 Configuração do servidor proxy

Se utilizar um servidor proxy para mediar a conexão com a Internet em um sistema utilizando o ESET Smart Security, ele deve ser especificado na Configuração avançada (F5). Para acessar a janela de configuração do **Servidor proxy**, clique em **Diversos > Servidor proxy**, em Configuração avançada. Selecione a caixa de seleção **Usar servidor proxy** e insira o endereço IP e a porta do servidor proxy, juntamente com os dados de autenticação.

Se essas informações não estiverem disponíveis, é possível tentar detectar automaticamente as configurações do servidor proxy para o ESET NOD32 Antivírus clicando no botão **Detectar servidor proxy**.

OBSERVAÇÃO: As opções de servidor proxy para diferentes perfis de atualização podem variar. Se este for o caso, configure o servidor proxy na configuração avançada de atualização.

3.4 Proteção de configurações

As Congurações do ESET NOD32 Antivírus podem ser muito importantes na perspectiva da política de segurança da sua organização. Modificações não autorizadas podem potencialmente pôr em risco a estabilidade e a proteção do seu sistema. Para proteger os parâmetros da configuração por senha, inicie no menu principal e clique em **Configuração > Entrar na configuração avançada... > Interface do usuário > Proteção de configurações** e clique no botão **Inserir senha...**

Insira uma senha, confirme-a digitando-a novamente e clique em **OK**. Essa senha será exigida para as modificações futuras nas configurações do ESET NOD32 Antivírus.

4. Trabalho com o ESET NOD32 Antivírus

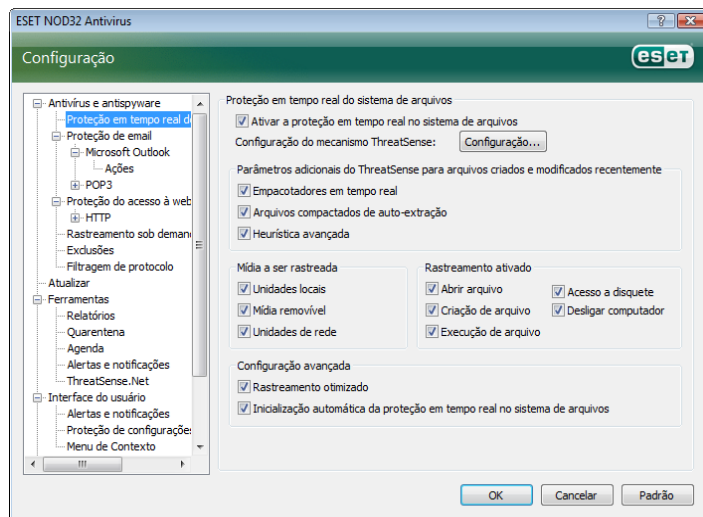
4.1 Proteção antivírus e antispyware

A proteção antivírus protege contra ataques de sistemas maliciosos ao controlar arquivos, e-mails e a comunicação pela Internet. Se uma ameaça for detectada, o módulo antivírus pode eliminá-la primeiro bloqueando-a e em seguida, limpando, excluindo ou movendo-a para a quarentena.

4.1.1 Proteção em tempo real do sistema de arquivos

A proteção em tempo real do sistema de arquivos controla todos os eventos do sistema relacionados a antivírus. Todos os arquivos são verificados quanto a código malicioso no momento em que são abertos, criados ou executados no computador. A proteção do sistema em tempo real é ativada na inicialização do sistema.

4.1.1.1 Configuração de controle

A proteção de sistema de arquivos em tempo real verifica todos os tipos de mídia e é acionada por vários eventos. O controle utiliza os métodos de detecção da tecnologia ThreatSense (conforme descrito em Configuração de parâmetros do mecanismo ThreatSense). O comportamento do controle em arquivos recém-criados e em arquivos existentes pode variar. Em arquivos recém-criados, é possível aplicar um nível mais profundo de controle.

4.1.1.1.1 Rastreamento de mídia

Por padrão, todos os tipos de mídia são rastreados quanto a ameaças potenciais.

Unidades locais – Controla todas as unidades de disco rígido do sistema
Mídia removível – Disquetes, dispositivos de armazenamento USB etc.
Unidades de rede – Rastreia todas as unidades mapeadas

Recomendamos manter as configurações padrão e modificá-las somente em casos específicos, como quando o rastreamento de determinada mídia tornar muito lenta a transferência de dados.

4.1.1.1.2 Rastreamento disparado por evento

Por padrão, todos os arquivos são verificados na abertura, execução ou criação. Recomendamos que você mantenha as configurações padrão, uma vez que estas fornecem o nível máximo de proteção em tempo real ao seu computador.

A opção **Acesso a disquete** providencia o controle do setor de inicialização do disquete quando essa unidade for acessada. A opção **Desligar computador** providencia o controle dos setores de inicialização do disco rígido durante o desligamento do computador. Embora os vírus de inicialização sejam raros atualmente, recomendamos deixar essas opções ativadas pois sempre há a possibilidade de infecção por um vírus de inicialização de origem alternativa.

4.1.1.1.3 Rastreamento de arquivos recém-criados

A probabilidade de infecção em arquivos recém-criados é comparativamente mais alta que nos arquivos já existentes. É por isso que o programa verifica esses arquivos com mais parâmetros de rastreamento. Juntamente com os métodos de rastreamento baseados em assinaturas comuns, é usada heurística avançada, que aumenta enormemente os índices de detecção. Além dos arquivos recém-criados, o rastreamento também é feito nos arquivos de extração automática (SFX) e nos empacotadores em tempo real (arquivos executáveis compactados internamente).

4.1.1.1.4 Configuração avançada

Para fornecer baixo impacto no sistema ao usar a proteção em tempo real, os arquivos já verificados não serão rastreados repetidamente (a menos que tenham sido modificados). Os arquivos são verificados novamente logo após cada atualização da base de dados de assinaturas de vírus. Esse comportamento é configurado utilizando a opção **Rastreamento otimizado**. Se esse recurso for desabilitado, todos os arquivos serão rastreados a cada vez que forem acessados.

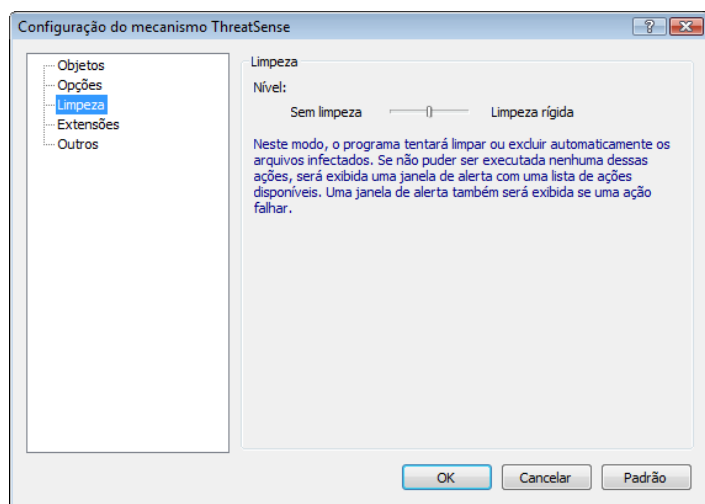
Por padrão, a proteção em tempo real é iniciada no momento da inicialização do sistema operacional, fornecendo rastreamento ininterrupto. Em casos especiais (por exemplo, se houver um conflito com outro rastreador em tempo real), a proteção em tempo real pode ser interrompida, desabilitando a opção **Inicialização automática da proteção em tempo real do sistema de arquivos**.

4.1.1.2 Níveis de limpeza

A proteção em tempo real possui três níveis de limpeza (para acessar, clique no botão **Configuração...** na seção **Proteção em tempo real do sistema de arquivos** e, em seguida, clique na ramificação **Limpeza**).

- O primeiro nível exibe uma janela de alerta com as opções disponíveis para cada ameaça encontrada. O usuário precisa escolher uma ação para cada ameaça individualmente. Esse nível é destinado aos usuários mais avançados que sabem o que fazer com cada tipo de ameaça.

- O nível médio escolhe e executa automaticamente uma ação predefinida (dependendo do tipo de ameaça). A detecção e a exclusão de um arquivo infectado são assinaladas por uma mensagem de informação localizada no canto inferior direito da tela. Entretanto, uma ação automática não é realizada se a infiltração estiver localizada dentro de um arquivo morto que também contenha arquivos limpos, e não será realizada em objetos para os quais não há ação predefinida.

- O terceiro nível é o mais "agressivo" – todos os objetos infectados são limpos. Uma vez que esse nível poderia potencialmente resultar em perda de arquivos válidos, recomendamos que seja usado somente em situações específicas.

4.1.1.3 Quando modificar a configuração da proteção em tempo real

A proteção em tempo real é o componente mais essencial para a manutenção de um sistema seguro. Portanto, seja cuidadoso ao modificar os parâmetros de proteção. Recomendamos que você modifique esses parâmetros apenas em casos específicos. Por exemplo, se houver um conflito com um certo aplicativo ou rastreador em tempo real de outro programa antivírus.

Após a instalação do ESET NOD32 Antivírus, todas as configurações serão otimizadas para fornecer o nível máximo de segurança do sistema para usuários. Para restaurar as configurações padrão, clique no botão **Padrão** localizado na parte inferior direita da janela **Proteção em tempo real do sistema de arquivos** (**Configuração avançada > Antivírus e antispyware > Proteção em tempo real do sistema de arquivos**).

4.1.1.4 Verificação da proteção em tempo real

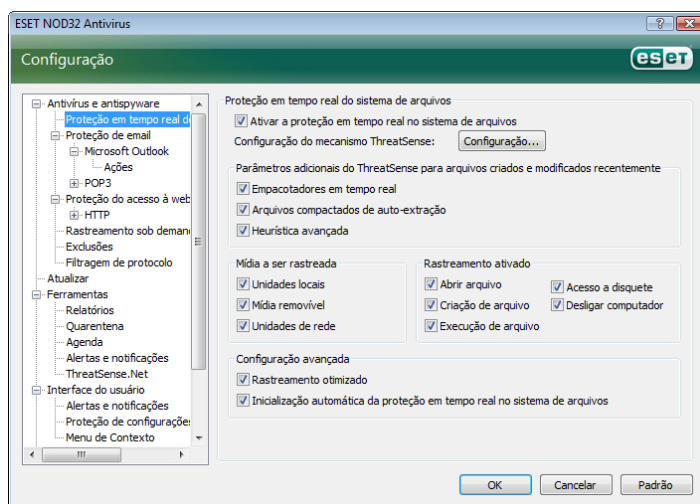
Para verificar se a proteção em tempo real está funcionando e detectando vírus, use um arquivo de teste do eicar.org. Este arquivo de teste é especial, inofensivo e detectável por todos os programas antivírus. O arquivo foi criado pela empresa EICAR (European Institute for Computer Antivirus Research) para testar a funcionalidade de programas antivírus. O arquivo eicar.com está disponível para download no endereço http://www.eicar.org/download/eicar.com

4.1.1.5 O que fazer se a proteção em tempo real não funcionar

No capítulo seguinte, descrevemos situações problemáticas que podem surgir quando usamos proteção em tempo real e como solucioná-las.

Proteção em tempo real desativada

Se a proteção em tempo real foi inadvertidamente desativada por um usuário, é preciso reativá-la. Para reativar a proteção em tempo real, navegue até **Configuração > Antivírus e antispyware** e clique em **Ativar** na seção **Proteção em tempo real do sistema de arquivos** da janela principal do programa.

Se a proteção em tempo real não for ativada na inicialização do sistema, isto provavelmente será devido à não ativação da opção **Inicialização automática da proteção em tempo real do sistema de arquivos**. Para ativar essa opção, navegue até **Configurações avançadas** (F5) e clique em **Proteção do sistema de arquivos em tempo real**, em Configuração avançada. Na seção **Configuração avançada** na parte inferior da janela, verifique se a caixa de seleção **Inicialização automática da proteção do sistema de arquivos em tempo real** está marcada.

A proteção em tempo real não detecta nem limpa infiltrações

Verifique se não há algum outro programa antivírus instalado no computador. Se duas proteções em tempo real forem ativadas ao mesmo tempo, elas podem entrar em conflito. Recomendamos desinstalar outros programas antivírus do sistema.

Proteção em tempo real não é iniciada

Se a proteção em tempo real não for ativada na inicialização do sistema (e estiver ativada a opção **Inicialização automática da proteção em tempo real do sistema de arquivos**), isto pode ser devido a conflitos com outros programas. Se for este o caso, consulte os especialistas do Serviço ao Cliente do ESET.

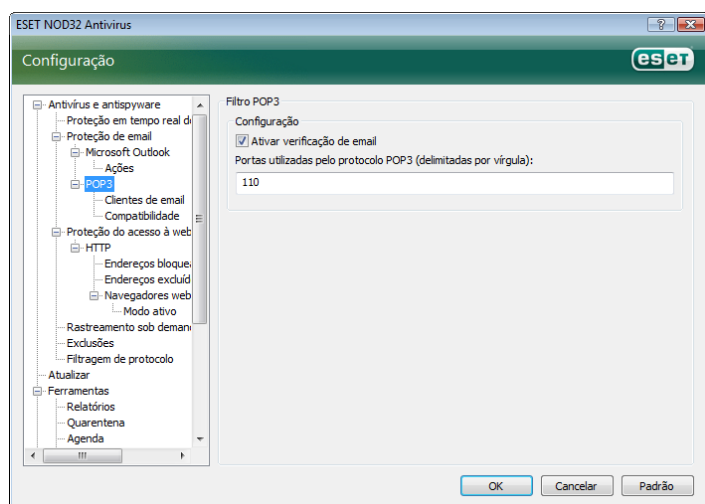
4.1.2 Proteção de e-mail

A proteção de e-mail fornece controle da comunicação por e-mail recebida via protocolo POP3. Com o plug-in para Microsoft Outlook, o ESET NOD32 Antivírus permite controlar todas as comunicações vindas através do cliente de e-mail (POP3, MAPI, IMAP, HTTP). Ao verificar as mensagens de entrada, o programa usa todos os métodos de rastreamento avançado fornecidos pelo mecanismo de rastreamento ThreatSense. Isto significa que a detecção de programas maliciosos é realizada até mesmo antes dos mesmos serem comparados com a base de dados de assinaturas de vírus. O rastreamento das comunicações via protocolo POP3 é independente do cliente de e-mail utilizado.

4.1.2.1 Verificação de POP3

O protocolo POP3 é o protocolo mais amplamente utilizado para receber mensagens em um cliente de e-mail. O ESET NOD32 Antivírus fornece proteção a esse protocolo, independentemente do cliente de e-mail usado.

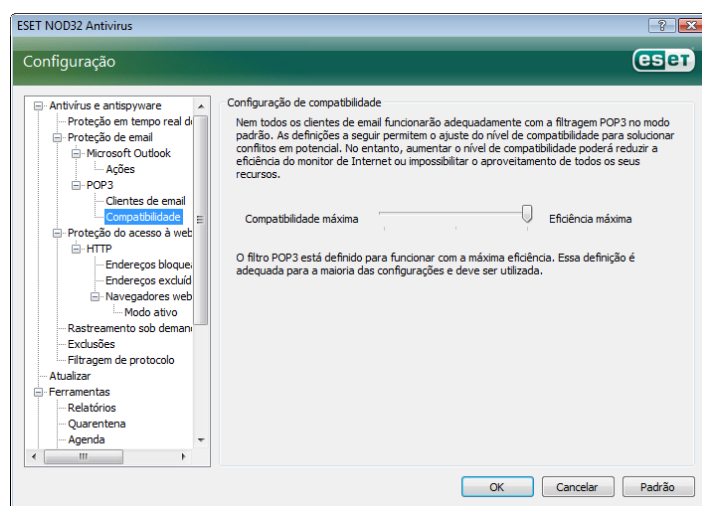
O módulo que permite esse controle é automaticamente ativado no momento da inicialização do sistema operacional e fica ativo na memória. Para que o módulo funcione corretamente, verifique se ele está ativado – o rastreamento do POP3 é feito automaticamente, sem necessidade de reconfiguração do cliente de e-mail. Por padrão, todas as comunicações através da porta 110 são rastreadas, mas podem ser adicionadas outras portas de comunicação, se necessário. Os números das portas devem ser delimitados por vírgula.

Não são controladas as comunicações codificadas.

4.1.2.1.1 Compatibilidade

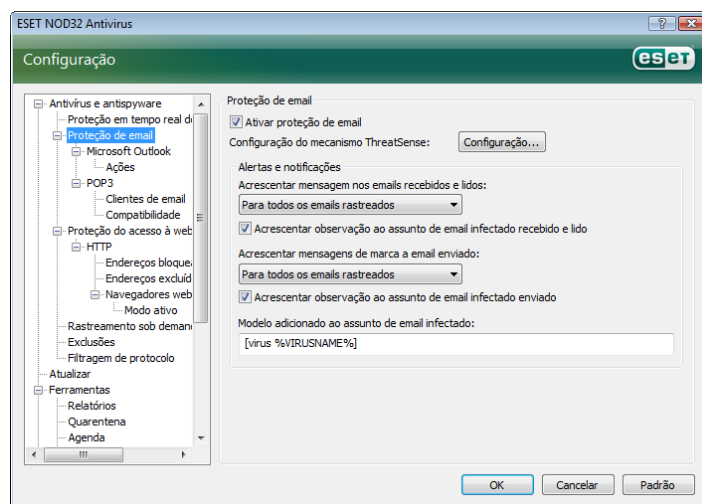
Certos programas de e-mail podem apresentar problemas com a filtragem POP3 (por exemplo, ao receber mensagens com uma conexão lenta de Internet, devido ao rastreamento pode ocorrer desativação por ultrapassar o limite de tempo). Se for este o caso, tente modificar a maneira como é feito o controle. A redução do nível de controle pode melhorar a velocidade do processo de limpeza. Para ajustar o nível de controle da filtragem POP3, navegue até **Antivírus e antispyware > Proteção de email > POP3 > Compatibilidade**.

Se for ativada a **Eficiência máxima**, as ameaças são removidas das mensagens infectadas e as informações sobre a ameaça serão inseridas na frente do assunto original do e-mail (as opções **Excluir** ou **Limpar** precisam estar ativadas ou o nível de limpeza **Rígida** ou **Padrão** precisa estar ativado)

Compatibilidade média modifica a maneira como as mensagens são recebidas. As mensagens são gradualmente enviadas ao cliente de e-mail. Após ser transferida a última parte da mensagem, ela será verificada quanto a ameaças. Contudo, o risco de infecção aumenta com esse nível de controle. O nível de limpeza e o processamento de mensagens de marca (alertas de notificação anexos à linha do assunto e corpo dos e-mails) são idênticos à configuração de eficiência máxima.

Com o nível **Compatibilidade máxima**, o usuário é avisado por uma janela de alerta, caso haja o recebimento de uma mensagem infectada. Não é adicionada nenhuma informação sobre arquivos infectados à linha do assunto ou ao corpo do e-mail de mensagens entregues e as ameaças não são automaticamente removidas. A exclusão de ameaças deve ser feita pelo usuário a partir do cliente de email.

4.1.2.2 Integração com o Microsoft Outlook, Outlook Express, Windows Mail

A integração do ESET NOD32 Antivírus com os clientes de e-mail aumenta o nível de proteção ativa contra códigos maliciosos em mensagens de e-mail. Se o seu cliente de e-mail for suportado, essa integração pode ser ativada no ESET Smart Security. Se a integração estiver ativada, os controles do ESET NOD32 Antivírus serão inseridos diretamente no cliente de e-mail, permitindo uma proteção mais eficiente de e-mail. As configurações de integração estão disponíveis utilizando **Configuração > Entrar na configuração avançada... > Diversos > Integração com clientes de e-mail**. Esta janela de diálogo permite ativar a integração com os clientes de e-mail suportados. Os clientes de e-mail que são atualmente suportados incluem o Microsoft Outlook, Outlook Express e o Windows Mail.

A proteção de e-mail é iniciada pela ativação da caixa de seleção **Ativar proteção de e-mail** em **Configuração avançada (F5)** > **Antivírus e antispyware** > **Proteção de e-mail**.

4.1.2.2.1 Anexar mensagens de marca ao corpo de um e-mail

Cada e-mail controlado pelo ESET NOD32 Antivírus pode ser marcado com uma mensagem, adicionada ao assunto ou ao corpo do e-mail. Esse recurso aumenta a credibilidade do endereço e, se alguma infiltração for detectada, ele fornece informações valiosas sobre o nível de ameaça de determinado e-mail/remetente.

As opções para essa funcionalidade estão disponíveis utilizando **Configuração avançada > Proteção antivírus e antispyware > Proteção de e-mail**. O programa pode **anexar mensagens para e-mails recebidos e lidos**, bem como **anexar mensagens a e-mails enviados**. Os usuários também podem decidir se as mensagens devem ser anexadas a todos os e-mails, somente aos e-mails infectados ou a nenhum e-mail.

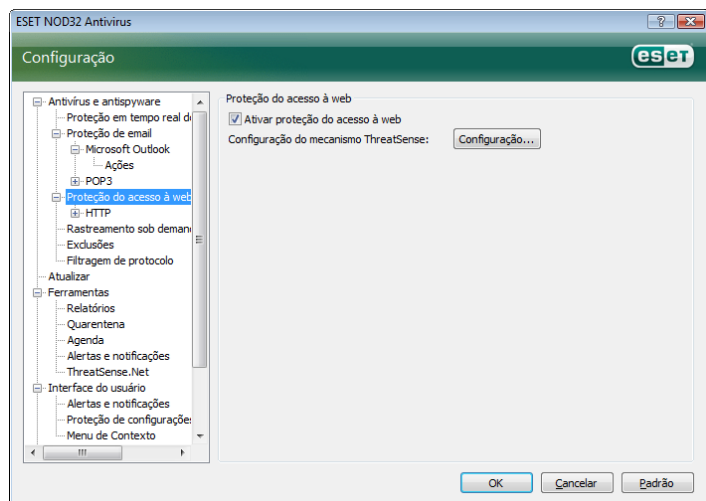
O ESET NOD32 Antivírus também permite ao usuário anexar mensagens ao assunto original das mensagens infectadas. Para permitir a anexação ao assunto, selecione as opções **Acrescentar observação ao assunto do e-mail infectado recebido e lido** e **Acrescentar observação ao assunto do e-mail infectado enviado**.

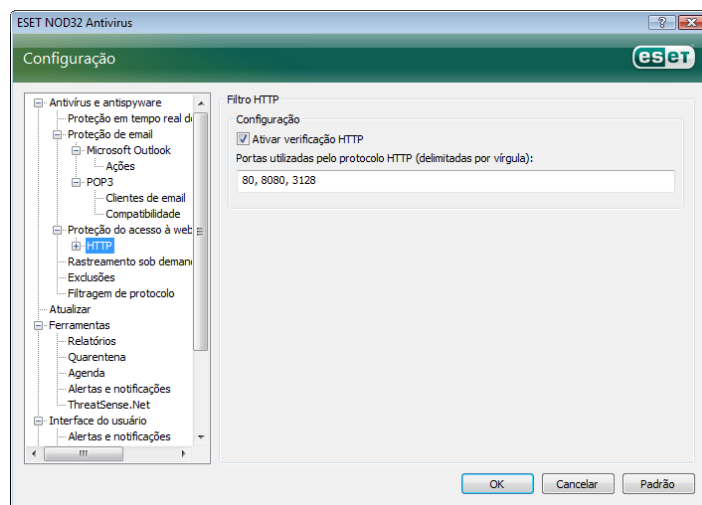
O conteúdo das notificações pode ser modificado no campo Modelo e acrescentado ao assunto do e-mail infectado. As modificações acima mencionadas podem ajudar a automatizar o processo de filtragem de e-mails infectados, uma vez que elas permitem que você filtre e-mails com um assunto específico (se suportado pelo seu cliente de e-mail) para uma pasta separada.

4.1.2.3 Remoção de infiltrações

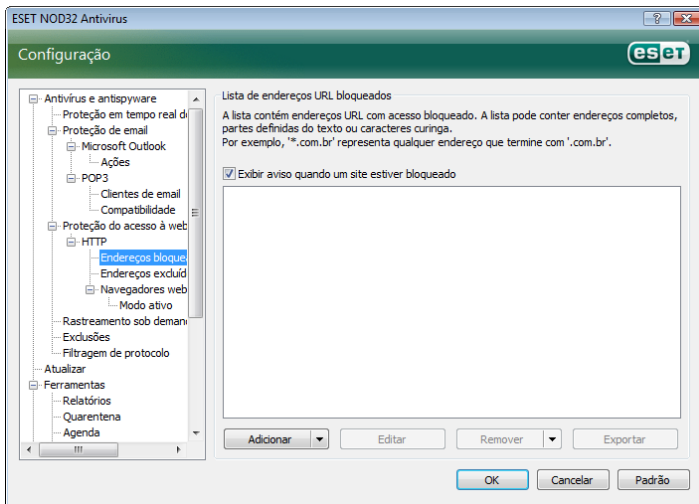
Se uma mensagem de e-mail infectada for recebida, uma janela de alerta será exibida. A janela de alerta mostra o nome do remetente, o e-mail e o nome da ameaça detectada. Na parte inferior da janela, as opções **Limpar**, **Excluir** ou **Deixar** estão disponíveis para o objeto detectado. Na maioria dos casos, recomendamos que você selecione **Limpar** ou **Excluir**. Em situações especiais, quando desejar receber o arquivo infectado, selecione **Deixar**. Se a **Limpeza rígida** estiver ativada, uma janela de informações sem nenhuma opção disponível para os objetos infectados será exibida.

4.1.3 Proteção de acesso à web

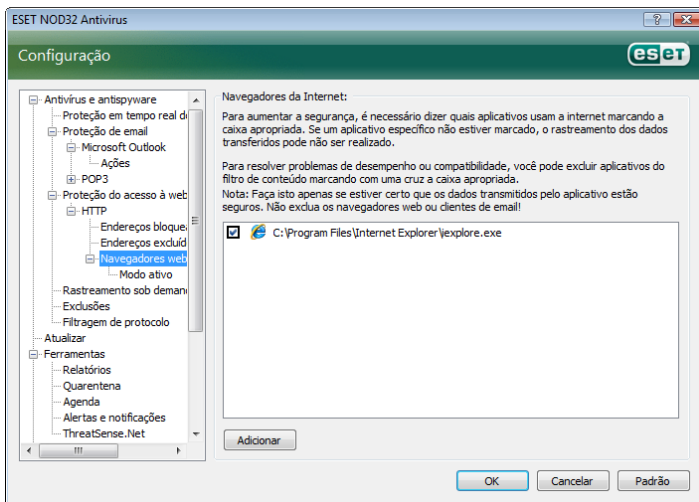
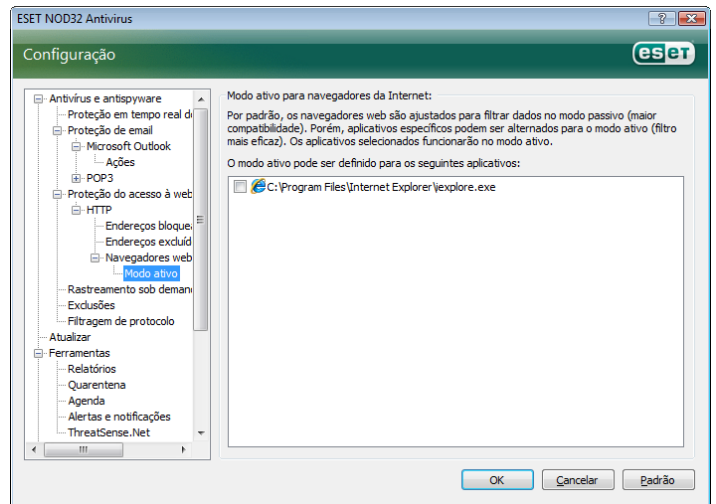
A conectividade com a Internet é um recurso padrão em um computador pessoal. Infelizmente, ela tornou-se o principal meio para transferência de códigos maliciosos. Por causa disso, é fundamental a atenta avaliação de sua proteção de acesso à web. Recomendamos que a opção **Ativar proteção do acesso à web** esteja ativada. Essa opção está localizada em **Configuração avançada (F5) > Proteção antivírus e antispyware > Proteção de acesso à web**.

4.1.3.1 HTTP

A principal função da Proteção de acesso à web é monitorar a comunicação entre os navegadores da Internet e os servidores remotos, de acordo com as regras do protocolo HTTP (Hypertext Transfer Protocol). O ESET NOD32 Antivírus está configurado, por padrão, para usar os padrões HTTP da maioria dos navegadores de Internet. Contudo, as opções de configuração do rastreamento de HTTP podem ser parcialmente modificadas na seção **Proteção de acesso à web > HTTP**. Na janela **Configuração de filtro HTTP**, é possível pode habilitar ou desabilitar o rastreamento do protocolo HTTP, usando a opção **Ativar verificação HTTP**. Você também pode definir os números das portas a serem usadas pelo sistema para estabelecer a comunicação HTTP. Por padrão, os números de portas 80, 8080 e 3128 são utilizados. O tráfego HTTP em qualquer porta pode ser automaticamente detectado e rastreado adicionando números de portas adicionais separados por uma vírgula.

4.1.3.1.1 Endereços excluídos/bloqueados

A configuração de verificação de HTTP permite criar listas definidas pelo usuário dos **endereços** de URL (Uniform Resource Locator) **Bloqueados** e **Excluídos**.

As duas janelas de diálogo contêm os botões **Adicionar**, **Editar**, **Remover** e **Exportar**, permitindo ao usuário gerenciar e manter facilmente as listas dos endereços especificados. Se um endereço solicitado pelo usuário estiver incluído na lista dos endereços bloqueados, não será possível acessar o endereço. Por outro lado, os endereços na lista dos endereços excluídos são acessados sem nenhum rastreamento de códigos maliciosos. Nas duas listas, os símbolos especiais * (asterisco) e **?** (ponto de interrogação) podem ser usados. O asterisco substitui qualquer string de caracteres, e o ponto de interrogação substitui qualquer símbolo. Tenha atenção especial ao especificar os endereços excluídos, uma vez que a lista deve conter os endereços seguros e confiáveis. De modo similar, é necessário verificar se os símbolos * e **?** são usados corretamente na lista.

4.1.3.1.2 Navegadores Web

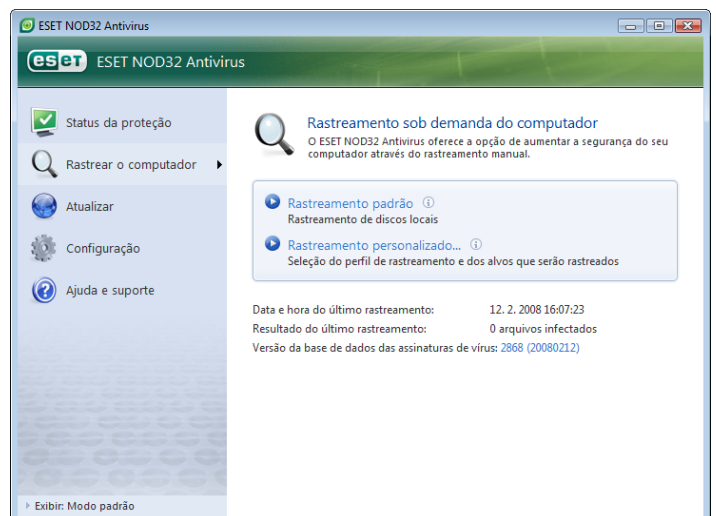
O ESET NOD32 Antivírus também contém o recurso **Navegadores Web**, que permite que o usuário defina se determinado aplicativo é um navegador ou não. Se um aplicativo for marcado como um navegador pelo usuário, todas as comunicações desse aplicativo serão monitoradas, independentemente do número de portas envolvidas na comunicação.

Os recursos dos navegadores Web complementam o recurso de verificação HTTP, uma vez que a verificação HTTP somente acontece nas portas predefinidas. Entretanto, muitos serviços da Internet utilizam alterações dinâmicas ou números de porta desconhecidos. Para levar isso em conta, o recurso do navegador Web pode estabelecer o controle das comunicações das portas, independentemente dos parâmetros da conexão.

A lista dos aplicativos marcados como navegadores pode ser acessada diretamente no submenu **Navegadores Web** de **HTTP**. Esta seção também contém o submenu **Modo Ativo**, que define o modo de verificação para os navegadores da Internet. O **Modo ativo** é útil porque ele examina os dados transferidos como um todo. Se não estiver ativado, a comunicação dos aplicativos é monitorada gradualmente em lotes. Isso diminui a eficiência do processo de verificação dos dados, mas também fornece compatibilidade mais alta para os aplicativos listados. Se nenhum problema ocorrer ao usá-lo, recomendamos que você ative o modo de verificação ativo marcando a caixa de seleção próxima ao aplicativo desejado.

4.1.4 Rastreamento do computador

Caso suspeite que seu computador esteja infectado (se ele se comportar de maneira anormal), execute um rastreamento sob demanda para examinar se há infiltrações no computador. Do ponto de vista da segurança, é fundamental que os rastreamentos do computador não sejam executados apenas quando há suspeita de uma infecção, mas regularmente como parte das medidas usuais de segurança. O rastreamento regular detecta infiltrações que não foram detectadas pelo rastreador em tempo real quando foram salvas no disco. Isto pode acontecer caso a proteção em tempo real esteja desativada no momento da infecção ou se a base de dados de assinatura de vírus estiver obsoleta.

Recomendamos executar um rastreamento sob demanda pelo menos uma ou duas vezes ao mês. O rastreamento pode ser configurado como uma tarefa programada em **Ferramentas > Agenda**.

4.1.4.1 Tipos de rastreamento

Dois tipos estão disponíveis. O **Rastreamento padrão** verifica rapidamente o sistema sem necessidade de mais configurações dos parâmetros de rastreamento. O **Rastreamento personalizado**... permite ao usuário selecionar qualquer perfil de rastreamento predefinido, bem como escolher os objetos do rastreamento na estrutura da árvore.

4.1.4.1.1 Rastreamento padrão

O Rastreamento padrão é um método amigável que permite ao usuário iniciar rapidamente um rastreamento no computador e limpar arquivos infectados sem a necessidade de intervenção do usuário. Suas principais vantagens são a operação fácil, sem configurações de rastreamento detalhadas. O Rastreamento padrão verifica todos os arquivos em unidades locais e limpa ou exclui automaticamente infiltrações detectadas. O nível de limpeza é automaticamente ajustado ao valor padrão. Para obter informações mais detalhadas sobre os tipos de limpeza, consulte Limpeza (consulte a página 18).

O perfil de rastreamento padrão foi elaborado para os usuários que desejam verificar de modo rápido e fácil seus computadores. Ele oferece um rastreamento eficiente e solução de limpeza sem exigir um extenso processo de configuração.

4.1.4.1.2 Rastreamento personalizado

O Rastreamento personalizado é uma solução excelente, caso queira especificar parâmetros de rastreamento adicionais, como rastreamento de destinos e métodos de rastreamento. A vantagem deste método é a capacidade de configurar os parâmetros detalhadamente. As configurações podem ser salvas nos perfis de rastreamento definidos pelo usuário, que podem ser úteis se o rastreamento for executado repetidamente com os mesmos parâmetros.

Para selecionar alvos de rastreamento, use o menu suspenso do recurso de seleção rápida de alvos ou selecione os alvos na estrutura em árvore que lista todos os dispositivos disponíveis no computador. Além disso, você pode selecionar entre três níveis de limpeza clicando em **Configuração... > Limpeza**. Caso esteja interessado unicamente em rastrear o sistema sem a realização de outras ações, marque a caixa de seleção **Rastrear sem limpar**.

A realização de rastreamentos de computador com o modo Rastreamento personalizado é adequada para usuários avançados com experiência anterior no uso de programas antivírus.

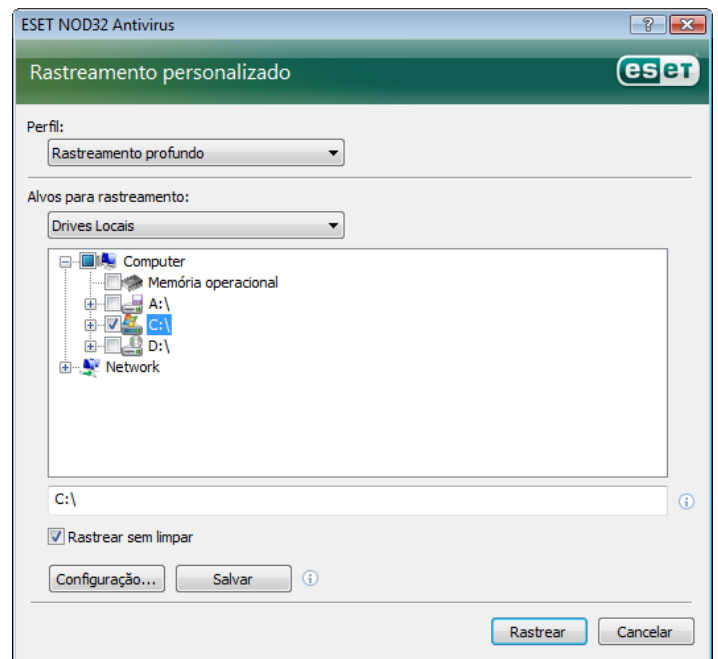
4.1.4.2 Alvos

O menu suspenso Alvos permite selecionar arquivos, pastas e dispositivos (discos) para rastreamento quanto a vírus.

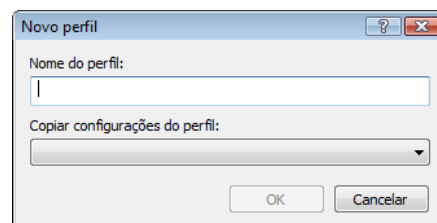
Com o uso do menu rápido Alvos para rastreamento, é possível selecionar os seguintes alvos:

Unidades locais – controla todas as unidades de disco rígido do sistema

Mídia removível – disquetes, dispositivos de armazenamento, CD/DVD

Unidades de rede – todas as unidades mapeadas

Um alvo para rastreamento também pode ser mais exatamente especificado através da inserção do caminho para a pasta ou arquivo(s) que você deseja incluir no rastreamento. Selecione alvos na estrutura em árvore que lista todos os dispositivos disponíveis no computador.

4.1.4.3 Perfis de rastreamento

Os parâmetros de rastreamento de computador preferidos podem ser salvos nos perfis. A vantagem de criar perfis de rastreamento é que eles podem ser usados regularmente para rastreamento futuro. Recomendamos a criação de tantos perfis (com diversas verificações de destino, métodos de rastreamento e outros parâmetros) quantos o usuário utilize regularmente.

Para criar um novo perfil que possa ser usado repetidamente em futuros rastreamentos, navegue até **Configuração avançada** (F5) **> Rastreamento sob demanda do computador**. Clique no botão **Perfis...** , à direita, para exibir a lista de perfis de rastreamento existentes e a opção para criar um novo perfil. A seguinte **Configuração de parâmetro do mecanismo ThreatSense** descreve cada parâmetro da configuração de rastreamento. Isto o ajudará a criar um perfil de rastreamento que atenda as suas necessidades.

Exemplo:
Imagine que você queira criar seu próprio perfil de rastreamento e que a configuração atribuída ao perfil **Smart Scan** seja parcialmente adequada. Mas você não deseja rastrear empacotadores em tempo real ou aplicativos potencialmente inseguros e você também deseja aplicar **Limpeza rígida**. Na janela **Perfis de configuração**, clique no botão **Adicionar...**. Insira o nome do seu novo perfil no campo **Nome do perfil** e selecione **Smart Scan** no menu suspenso **Copiar configurações do perfil:**. Depois, ajuste os demais parâmetros de maneira que atender às suas necessidades.

4.1.5 Configuração do mecanismo ThreatSense

ThreatSense é o nome da tecnologia que consiste em métodos complexos de detecção de ameaças. Essa tecnologia é proativa, o que significa que ela também fornece proteção durante as primeiras horas da propagação de uma nova ameaça. Ela utiliza uma combinação de diversos métodos (análise de código, emulação de código, assinaturas genéricas e assinaturas de vírus) que funcionam em conjunto para otimizar significativamente a segurança do sistema. O mecanismo de rastreamento é capaz de controlar diversos fluxos de dados simultaneamente, maximizando a eficiência e a taxa de detecção. A tecnologia ThreatSense também elimina com êxito os rootkits.

As opções de configuração da tecnologia ThreatSense permitem que o usuário especifique diversos parâmetros de rastreamento:

- Tipos e extensões de arquivos que serão rastreados
- A combinação de diversos métodos de detecção
- Níveis de limpeza etc.

Para entrar na janela de configuração, clique no botão **Configuração...** localizado na janela de configuração de qualquer módulo que utiliza a tecnologia ThreatSense (consulte a seguir). Cenários de segurança diferentes podem requerer configurações diferentes. Com isto em mente, o ThreatSense pode ser configurado individualmente para os seguintes módulos de proteção:

- Proteção em tempo real do sistema de arquivos
- Rastrear arquivos na inicialização do sistema
- Proteção de e-mail
- Proteção de acesso à web
- Rastreamento sob demanda do computador

Os parâmetros do ThreatSense são altamente otimizados para cada módulo e a modificação deles pode influenciar significativamente a operação do sistema. Por exemplo, alterar parâmetros para sempre rastrear empacotadores em tempo real ou ativar heurística avançada no módulo de proteção do sistema de arquivos em tempo real pode resultar em redução da velocidade do sistema (normalmente, somente arquivos recém-criados são rastreados utilizando esses métodos). Portanto, recomendamos que mantenha os parâmetros padrão do ThreatSense inalterados para todos os módulos, exceto o módulo Rastrear o computador.

4.1.5.1 Configuração dos objetos

A seção **Objetos** permite definir quais componentes do computador e arquivos serão verificados quanto a infiltrações.

Memória operacional – Rastreia quanto a ameaças que atacam a memória operacional do sistema.

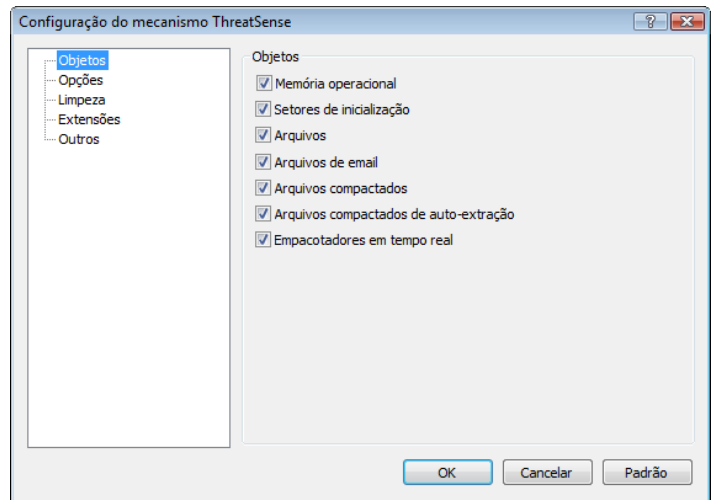
Setores de inicialização – Rastreia os setores de inicialização quanto à presença de vírus no registro principal de inicialização

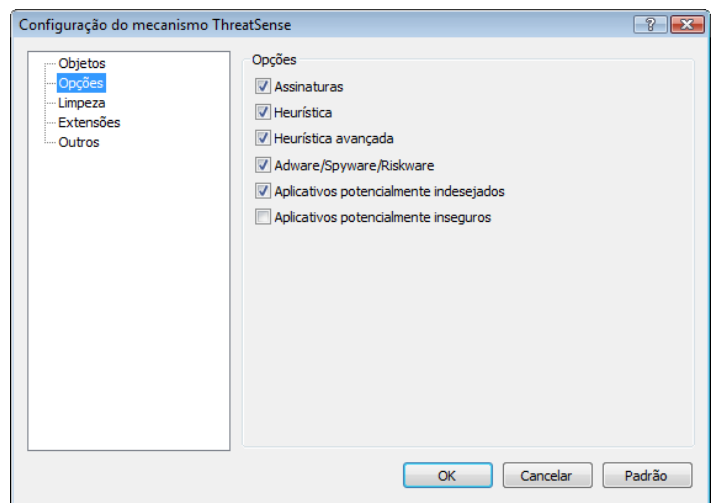
Arquivos – Fornece o rastreamento de todos os tipos de arquivos comuns (programas, imagens, áudio, arquivos de vídeo, arquivos de base de dados etc.)

Arquivos de e-mail – Rastreia arquivos especiais que contêm mensagens de e-mail

Arquivos mortos – Fornece o rastreamento dos arquivos compactados em arquivos mortos (.rar, .zip, .arj, .tar etc.)

Arquivos de extração automática – Rastreia arquivos contidos em arquivos mortos de extração automática, mas que usualmente possuem a extensão

Empacotadores em tempo real – os empacotadores em tempo real (diferente dos tipos de arquivo padrão) são descompactados na memória, além de empacotadores estáticos padrão (UPX, yoda, ASPack, FGS etc.).

4.1.5.2 Opções

Na seção **Opções**, o usuário pode selecionar os métodos a serem usados quando rastrear o sistema buscando infiltrações. Estão disponíveis as seguintes opções:

Assinaturas – As assinaturas podem detectar e identificar infiltrações pelo nome, com exatidão e confiabilidade, usando as assinaturas de vírus.

Heurística – A heurística é um algoritmo que analisa a atividade (maliciosa) de programas. A principal vantagem da detecção heurística é a capacidade de detectar novos softwares maliciosos, que não existiam antes ou não estavam incluídos na lista de vírus conhecidos (base de dados de assinaturas de vírus).

Heurística avançada – A heurística avançada é formada por um algoritmo heurístico exclusivo, desenvolvido pela ESET e otimizado para a detecção de vírus e cavalos de tróia de computador escritos em linguagens de programação de alto nível. Devido à heurística avançada, a inteligência de detecção do programa é significativamente maior.

Adware/Spyware/Riskware – Esta categoria inclui software que coleta várias informações sensíveis sobre usuários sem conhecimento ou consentimento dos mesmos. E inclui, ainda, software que exibe material de propaganda.

Aplicativos potencialmente não seguros – Aplicativos potencialmente não seguros é a classificação usada para software comercial legítimo. Inclui programas como ferramentas de acesso remoto, motivo pelo qual essa opção, por padrão, é desativada.

Aplicativos potencialmente não desejados – Aplicativos potencialmente não desejados não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de maneira negativa. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são janelas pop-up indesejadas, ativação e execução de processos ocultos, aumento do uso de recursos do sistema, modificações nos resultados de pesquisa e aplicativos se comunicando com servidores remotos.

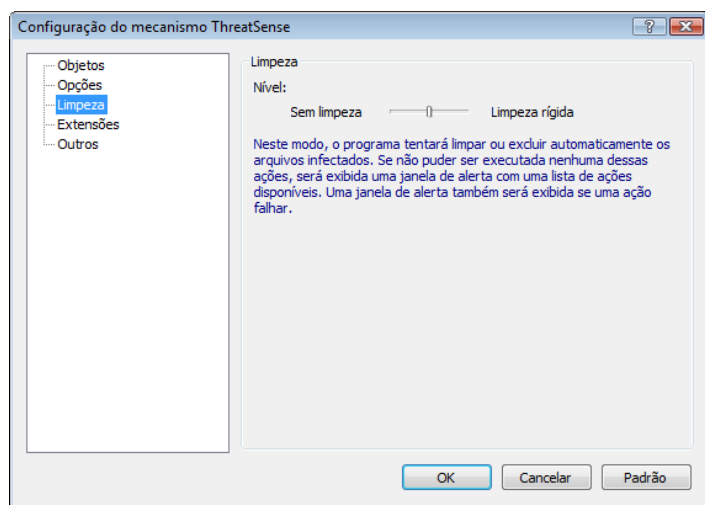
4.1.5.3 Limpeza

As configurações de limpeza determinam o comportamento do rastreador durante a limpeza dos arquivos infectados. Há três níveis de limpeza:

Sem limpeza
Os arquivos infectados não são limpos automaticamente. O programa exibirá uma janela de aviso e permitirá que o usuário escolha uma ação.

Nível padrão
O programa tentará limpar ou excluir automaticamente um arquivo infectado. Se não for possível, para selecionar a ação correta automaticamente, o programa oferecerá uma escolha de ações a seguir. A escolha das ações a seguir também será exibida se uma ação predefinida não for concluída.

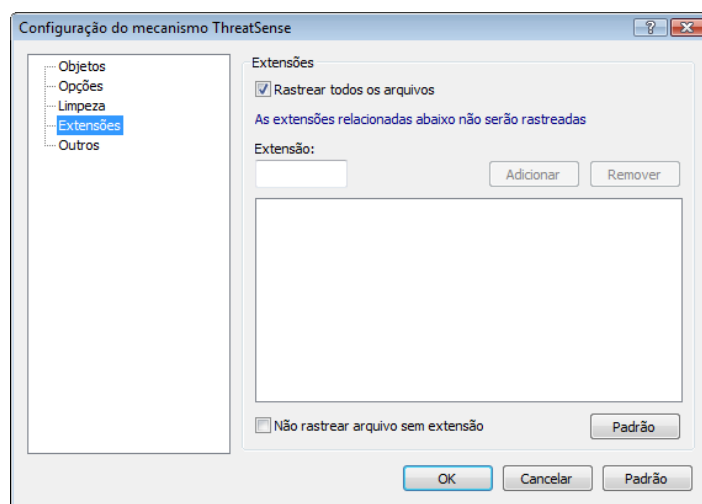
Limpeza rígida
O programa limpará ou excluirá todos os arquivos infectados (incluindo os arquivos mortos). As únicas exceções são os arquivos do sistema. Se não for possível limpá-los, uma ação a ser tomada será sugerida ao usuário em uma janela de aviso.

Aviso:
No modo Padrão, todo arquivo morto será excluído somente se todos os arquivos no arquivo morto infectado estiverem infectados. Se o arquivo morto contiver arquivos legítimos, ele não será excluído. Se um arquivo morto infectado for detectado no modo Limpeza rígida, todo arquivo morto será excluído, mesmo se arquivos limpos estiverem presentes.

4.1.5.4 Extensões

Extensão é a parte do nome de arquivo delimitada por um ponto final. A extensão define o tipo e o conteúdo do arquivo. Esta seção de configuração de parâmetros do ThreatSense permite definir os tipos de arquivos a serem rastreados.

Por padrão, todos os arquivos são rastreados, independentemente de suas extensões. Qualquer extensão pode ser adicionada à lista de arquivos excluídos do rastreamento. Se a opção **Rastrear todos os arquivos** não estiver marcada, a lista é alterada para mostrar todos as extensões de arquivo rastreadas no momento. Com os botões **Adicionar** e **Remover**, você pode habilitar ou desabilitar o rastreamento das extensões desejadas.

Para habilitar o rastreamento de arquivos sem nenhuma extensão, selecione a opção **Rastrear arquivos sem extensão**.

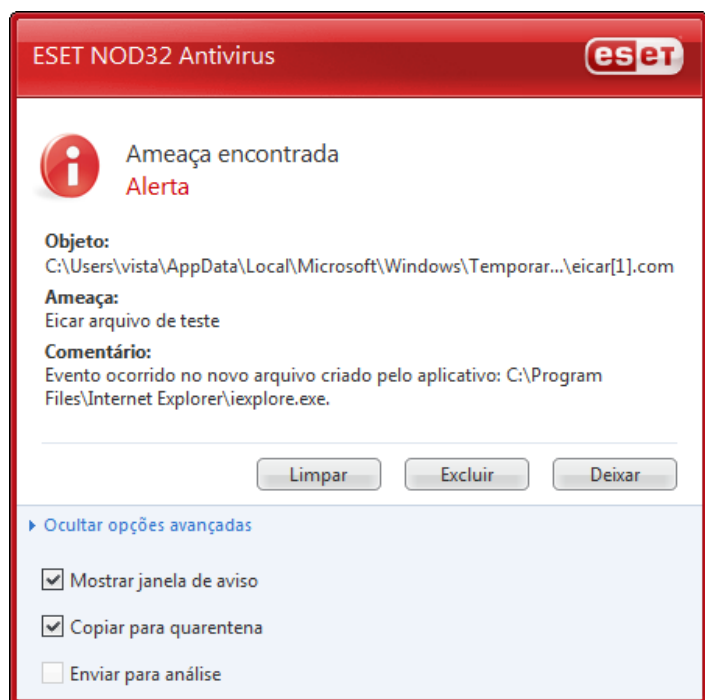
A exclusão de arquivos do rastreamento pode ser útil se o rastreamento de determinados tipos de arquivos provocar a operação incorreta do programa que usa as extensões. Por exemplo, você poderá ser aconselhado a excluir as extensões EDB, EML e TMP se usar o servidor MS Exchange.

4.1.6 Uma infiltração foi detectada

As infiltrações podem alcançar o sistema a partir de vários pontos: páginas da web, arquivos compartilhados, e-mail ou dispositivos removíveis (USB, discos externos, CDs, DVDs, disquetes, etc.)

Se o seu computador estiver apresentando sinais de mau funcionamentos, por exemplo, estiver mais lento, travar com freqüência, recomendamos que você faça o seguinte:

- Abra o ESET NOD32 Antivírus e clique em **Rastrear o Computador**
- Clique no botão Rastreamento padrão (para obter mais informações, consulte Rastreamento padrão).
- Após o rastreamento ter terminado, revise o relatório para informações como número dos arquivos verificados, infectados e limpos.

Se desejar apenas verificar uma parte do seu disco, clique em **Rastreamento personalizado** e selecione os alvos a serem verificados quanto a vírus.

Como exemplo geral de como as ameaças são manuseadas no ESET Smart Security, suponha que uma ameaça seja detectada pelo monitor do sistema de arquivo em tempo real, que usa o nível de limpeza Padrão. Ele tentará limpar ou excluir o arquivo. Se não houver uma ação predefinida a ser tomada para o módulo de proteção em tempo real, será solicitado a você que selecione uma opção na janela de alerta. Geralmente as opções **Limpar**, **Excluir** e **Deixar** estão disponíveis. A seleção da opção **Deixar** não é recomendada, visto que os arquivos infectados são deixados intocados. A exceção a isso é quando você tem certeza de que o arquivo é inofensivo e foi detectado por engano.

Limpeza e exclusão
Aplique a limpeza se um arquivo limpo tiver sido atacado por um vírus que anexou um código malicioso a esse arquivo limpo. Se esse for o caso, tente primeiro limpar o arquivo infectado a fim de restaurá-lo ao seu estado original. Se o arquivo for constituído exclusivamente por código malicioso, ele será excluído.

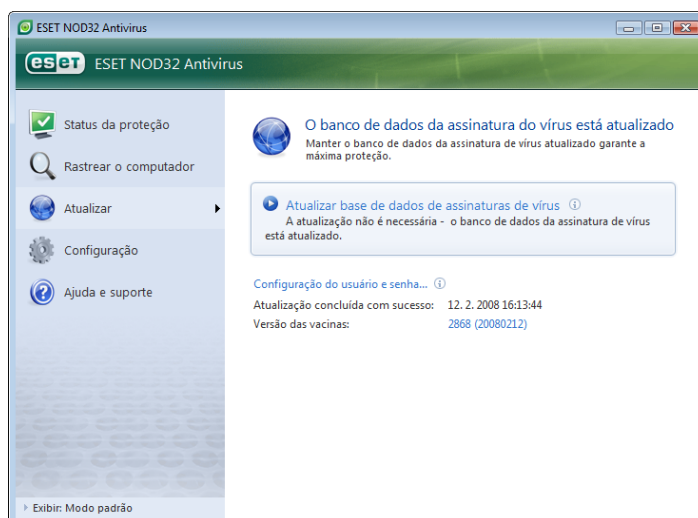
Se um arquivo infectado estiver "bloqueado" ou em uso pelo processo do sistema, ele somente será excluído após ter sido liberado (geralmente após a reinicialização do sistema).

Exclusão de arquivos em arquivos mortos
No modo de limpeza Padrão, os arquivos mortos serão excluídos somente se contiverem arquivos infectados e nenhum arquivo limpo. Em outras palavras, os arquivos mortos não são excluídos se eles também contiverem arquivos limpos inofensivos. Entretanto, tome cuidado ao realizar um rastreamento de Limpeza rígida – com esse tipo de limpeza o arquivo será excluído se ele contiver pelo menos um arquivo infectado, independentemente do status dos demais arquivos contidos no arquivo morto.

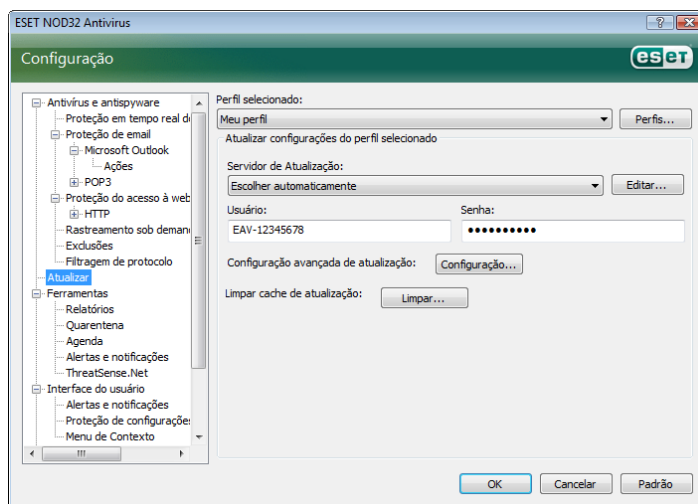
4.2 Atualização do programa

A atualização regular do sistema é o princípio básico para obter o nível máximo de segurança fornecido pelo ESET Smart Security. O módulo de atualização garante que o programa estará sempre atualizado. Isso é feito de duas maneiras: atualizando a base de dados de assinatura de vírus e atualizando todos os componentes do sistema.

As informações sobre o status atual da atualização podem ser encontradas clicando em **Atualizar**, incluindo a versão atual da base de dados de assinatura de vírus e se uma atualização será exigida. Além disso, a opção para ativar o processo imediato da atualização – **Atualizar base de dados de assinatura de vírus** – está disponível, bem como as opções básicas de configuração de atualização, como, por exemplo, o nome do usuário e a senha para acessar os servidores de atualização da ESET.

A janela de informações também contém detalhes, como a data e hora da última atualização bem-sucedida e o número da base de dados da assinatura de vírus. Esta indicação numérica é um link ativo para o site da ESET na Web que lista todas as assinaturas adicionadas dentro da atualização específica.

OBSERVAÇÃO: O Usuário e a Senha são fornecidos pelo ESET após a compra do ESET Smart Security.

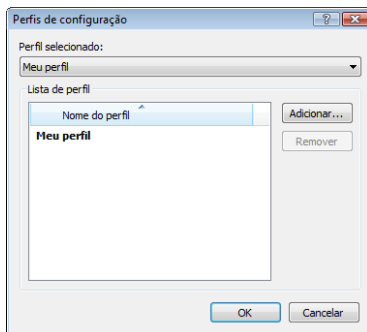
4.2.1 Configuração da atualização

Na seção de configuração da atualização você especifica as configurações da atualização, por exemplo, os servidores de atualização e os dados de autenticação para esses servidores. Por padrão, o campo **Atualizar servidor:** está configurado como **Escolher automaticamente**. Esse valor assegura que será feito o download dos arquivos de atualização automaticamente a partir do servidor ESET com a menor carga de tráfego de rede. As opções de configuração da atualização estão disponíveis em Configuração avançada (F5) , em **Atualizar**.

A lista de servidores de atualização existentes no momento pode ser acessada utilizando o menu suspenso **Atualizar servidor:**. Para adicionar um novo servidor de atualização, clique em **Editar** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**.

A autenticação nos servidores de atualização é garantida através do **Nome de usuário** e **Senha** que foram gerados e enviados pela ESET para o usuário após a compra da licença do produto.

4.2.1.1 Atualizar perfis

Para várias configurações de atualização, é possível criar perfis de atualização, definidos pelo usuário, que podem ser utilizados para determinada tarefa de atualização. A criação de vários perfis de atualização é especialmente útil para usuários móveis, uma vez que as propriedades de conexão à Internet mudam regularmente. Ao modificarem a tarefa de atualização, os usuários móveis podem especificar que, se não for possível atualizar o programa utilizando a configuração especificada em **Meu perfil**, a atualização será executada utilizando um perfil alternativo.

O menu suspenso **Perfil selecionado** exibe o perfil selecionado no momento. Por padrão, essa entrada é configurada como **Meu perfil**. Para criar um novo perfil, clique no botão **Perfis...** e, em seguida, clique no botão **Adicionar...** e insira seu próprio **Nome de perfil**. Ao criar um novo perfil, é possível copiar as configurações de um perfil existente selecionando-o no menu suspenso **Copiar configurações do perfil:**.

Dentro da configuração do perfil, é possível especificar o servidor de atualização ao qual o programa se conectará e fazer download de atualizações; qualquer servidor da lista de servidores disponíveis pode ser utilizado ou um novo servidor pode ser adicionado. A lista de servidores de atualização existentes pode ser acessada utilizando o menu suspenso **Atualizar servidor:**. Para adicionar um novo servidor de atualização, clique em **Editar...** na seção **Atualizar configurações de perfil selecionado** e, em seguida, clique no botão **Adicionar**.

4.2.1.2 Configuração avançada de atualização

Para exibir a opção **Configuração avançada de atualização**, clique no botão **Configuração...**. As opções de configuração avançada de atualização incluem a configuração de **Modo de atualização, Proxy HTTP, LAN** e **Imagem**.

4.2.1.2.1 Modo de atualização

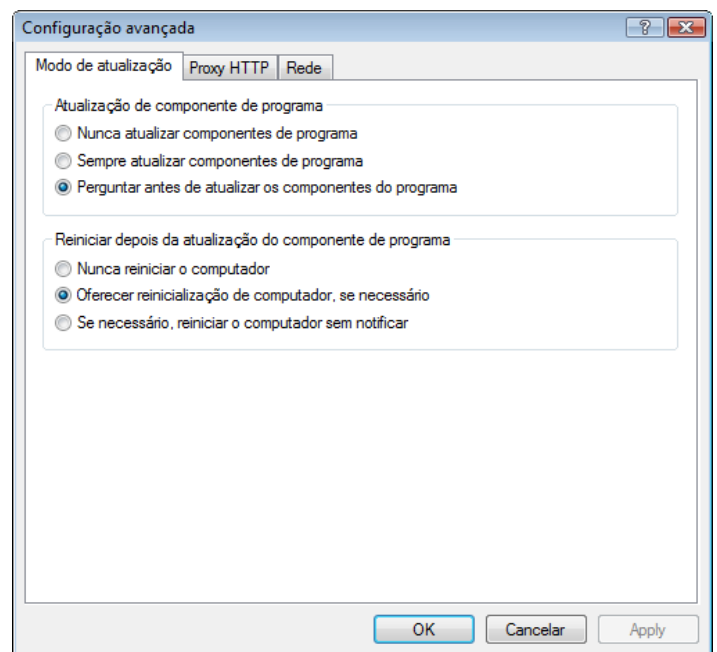
A guia **Modo de atualização** contém opções relacionadas à atualização do componente do programa.

Na seção **Atualização de componente de programa**, três opções estão disponíveis:

- **Nunca atualizar componentes de programa**
- **Sempre atualizar componentes de programa**
- **Perguntar antes de fazer download dos componentes de programa**

A escolha da opção **Nunca atualizar componentes de programa** garante que não será feito o download de uma nova atualização de componentes do programa liberados pelo ESET, e nenhuma atualização do componente de programa ocorrerá realmente na estação de trabalho. A opção **Sempre atualizar componentes de programa** significa que as atualizações do componente de programa serão executadas toda vez que uma nova atualização estiver disponível nos servidores de atualização do ESET e que os componentes do programa serão atualizados para a versão cujo download foi feito.

Selecione a terceira opção **Perguntar antes de fazer download dos componentes de programa** para garantir que o programa solicitará ao usuário a confirmação para iniciar o download das atualizações de componente do programa no momento em que essas atualizações estiverem disponíveis. Neste caso, uma janela de diálogo que contém informações sobre as atualizações do componente de programa será exibida com a opção de confirmação ou de recusa. Se confirmada, será feito o download das atualizações e os novos componentes do programa serão instalados.

A opção padrão para a atualização do componente de programa é **Perguntar antes de fazer download dos componentes de programa**.

Após a instalação de uma atualização de componente do programa, é necessário reiniciar o sistema para uma completa funcionalidade de todos os módulos. A seção **Reiniciar depois da atualização do componente de programa** permite que o usuário selecione uma das três opções a seguir:

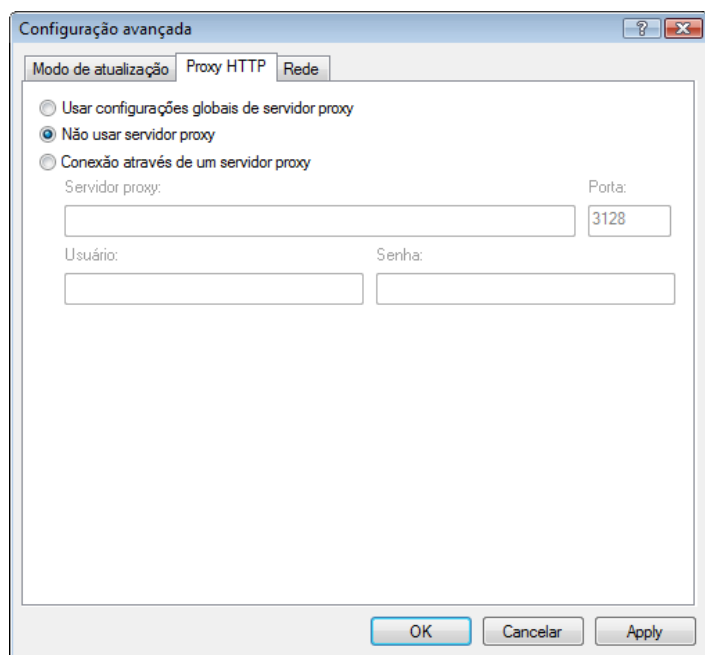
- **Nunca reiniciar o computador**
- **Sugerir opção de reinicialização do computador, se necessário**
- **Se necessário, reinicialize o computador sem notificação.**

A opção padrão para reiniciar é **Sugerir opção de reinicialização do computador, se necessário**. A escolha das opções mais apropriadas para as atualizações de componente do programa na guia **Modo de atualização** depende de cada estação de trabalho e/ou usuário(s) e conforme o local onde as configurações serão aplicadas. Esteja ciente de que há diferenças entre estações de trabalho e servidores; por exemplo, reiniciar o servidor automaticamente após uma atualização de programa pode provocar danos sérios.

4.2.1.2.2 Servidor proxy

Para acessar as opções de configuração do servidor proxy para determinado perfil de atualização: Clique em **Atualizar**, em Configuração avançada (F5), e, em seguida, clique no botão **Configuração...**, à direita de **Configuração avançada de atualização.** Clique na guia **Proxy HTTP** e selecione uma das três opções a seguir:

- **Usar configurações globais de servidor proxy**
- **Não usar servidor proxy**
- **Conexão através de um servidor proxy** (conexão definida pelas propriedades de conexão)

A seleção da opção **Usar configurações globais de servidor proxy** utilizará as opções de configuração do servidor proxy já especificadas dentro de **Diversos > Servidor proxy**, em Configuração avançada.

Selecione a opção **Não usar servidor proxy** para definir explicitamente que nenhum servidor proxy será utilizado para atualizar o ESET Smart Security.

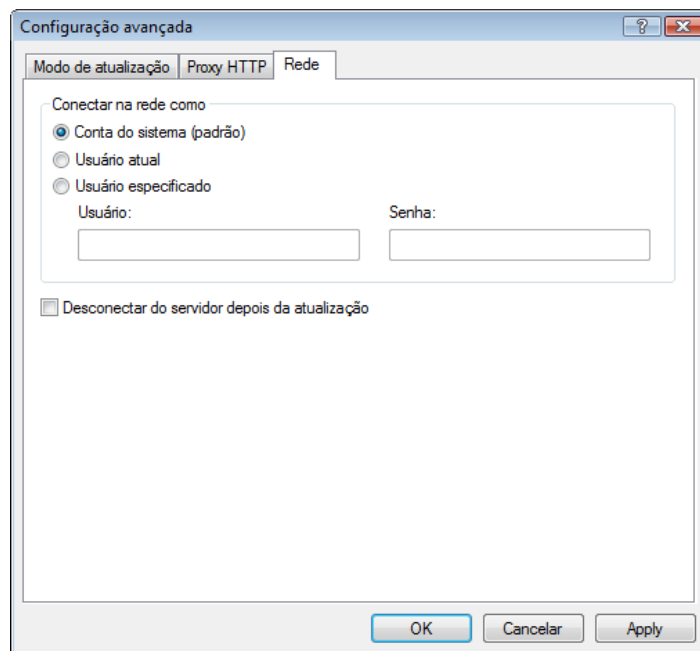
A opção **Conexão através de um servidor proxy** deve ser escolhida se um servidor proxy é para ser utilizado para atualizar o ESET NOD32 Antivírus e for diferente do servidor proxy especificado nas configurações globais (**Diversos > Servidor proxy**). Se for escolhida, as configurações devem ser especificadas aqui: endereço do **Servidor proxy**, **Porta** de comunicação, além de **Nome de usuário** e **Senha** para o servidor proxy se necessário.

Essa opção também deve ser selecionada se as configurações do servidor proxy não foram configuradas globalmente, mas o ESET NOD32 Antivírus se conectará a um servidor proxy para atualizações.

A configuração padrão para o servidor proxy é **Usar configurações globais de servidor proxy**.

4.2.1.2.3 Conexão à rede

Ao atualizar a partir de um servidor local com um sistema operacional baseado em NT, a autenticação para cada conexão de rede é necessária por padrão. Na maioria dos casos, uma conta do sistema local não tem direitos de acesso suficientes para a pasta Imagem que contém cópias dos arquivos de atualização. Se este for o caso, insira o nome de usuário e senha na seção de configuração da atualização ou especifique uma conta existente na qual o programa acessará o servidor de atualização (Imagem).

Para configurar essa conexão, clique na guia **Rede**. A seção **Conectar na rede como** apresenta as opções **Conta do sistema (padrão)**, **Usuário atual** e **Usuário especificado**.

Selecione a opção **Conta do sistema** para utilizar a conta do sistema para autenticação. Normalmente, nenhum processo de autenticação ocorrerá se não houver nenhum dado de autenticação fornecido na seção principal de configuração de atualização.

Para garantir que o programa autorize a si próprio utilizando uma conta de usuário que tiver feito logon no momento, selecione **Usuário atual**. A desvantagem dessa solução é que o programa não é capaz de conectar-se a o servidor de atualização se nenhum usuário tiver feito logon no momento.

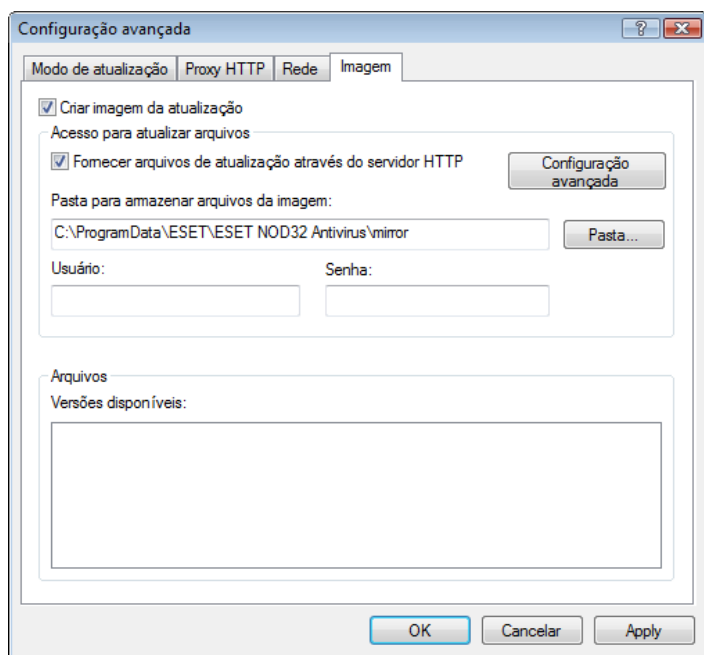
Selecione **Usuário especificado** se desejar que o programa utilize uma conta de usuário específica para autenticação.

A opção padrão para a conexão na rede é **Conta do sistema**.

Aviso:
Quando a opção **Usuário atual** ou **Usuário especificado** estiver ativada, um erro pode ocorrer ao alterar a identidade do programa para o usuário desejado. Por isso recomendamos a inserção de dados de autenticação na rede na seção principal de configuração da atualização. Nesta seção de configuração da atualização, os dados de autenticação devem ser inseridos da seguinte maneira: nome_domínio\usuário (se for um grupo de trabalho, insira grupo trabalho_nome\nome) e a senha do usuário. Ao atualizar da versão HTTP do servidor local, nenhuma autenticação é necessária.

4.2.1.2.4 Criação de cópias de atualização – Imagem

O ESET NOD32 Antivírus Business Edition permite que o usuário crie cópias dos arquivos de atualização que podem ser utilizadas para atualizar outras estações de trabalho localizadas na rede. A atualização das estações de cliente a partir de uma Imagem otimiza o equilíbrio de carga da rede e economiza a largura de banda da conexão com a Internet.

As opções de configuração para a Imagem do servidor local podem ser acessadas (após adicionar uma chave de licença no gerenciador de licenças, localizado na seção Configuração avançada do ESET Smart Security Business Edition) na seção **Configuração avançada de atualização:** (para acessar essa seção, pressione F5 e clique em **Atualizar**, em Configuração avançada. Clique no botão **Configuração...** próximo à opção **Configuração avançada de atualização:** e selecione a guia **Imagem**).

A primeira etapa na configuração da Imagem é marcar a caixa de seleção **Criar imagem da atualização**. A seleção dessa opção ativa as outras opções de configuração da Imagem, como o modo em que os arquivos serão acessados e o caminho de atualização para os arquivos da imagem.

Os métodos de ativação da Imagem são descritos em detalhes no próximo capítulo, "Variantes de acesso à Imagem". Por enquanto, observe que há duas variantes básicas de acesso à Imagem: a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

A pasta dedicada a armazenar os arquivos de atualização para a imagem é definida na seção **Pasta para armazenar arquivos da imagem**. Clique em **Pasta...** para procurar uma pasta desejada no computador local ou uma pasta de rede compartilhada. Se a autorização para a pasta especificada for necessária, os dados de autenticação devem ser fornecidos nos campos **Nome do usuário** e **Senha**. O Nome do usuário e a Senha devem ser inseridos no formato *Domínio/Usuário* ou *Grupo de trabalho/Usuário*. Lembre-se de fornecer as senhas correspondentes.

Ao especificar a configuração da imagem detalhada, você também pode especificar as versões de idioma dos quais deseja fazer download das cópias de atualização. A configuração da versão de idioma pode ser acessada na seção **Arquivos > Versões disponíveis**.

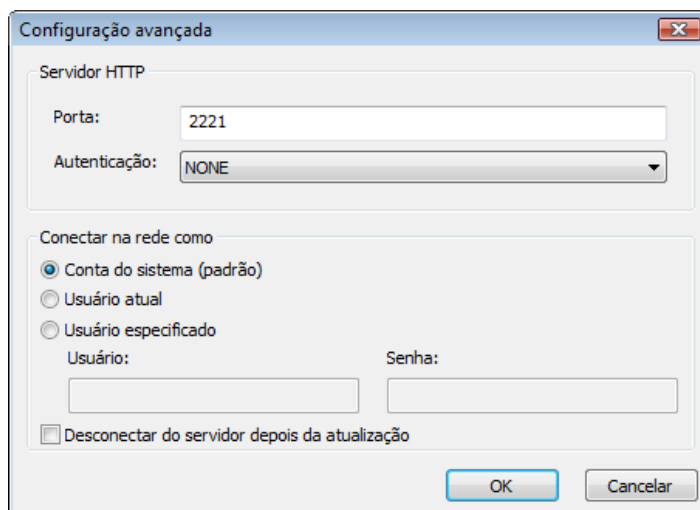
4.2.1.2.4.1 Atualização através da Imagem

Há dois métodos básicos de configuração da Imagem: a pasta com os arquivos de atualização pode ser apresentada como uma pasta de rede compartilhada ou através de um servidor HTTP.

Acesso à Imagem utilizando um servidor HTTP interno

Esta configuração é a padrão, especificada na configuração de programa predefinida. Para permitir acesso à Imagem utilizando um servidor HTTP, navegue até **Configuração avançada de atualização** (a guia **Imagem**) e selecione a opção **Criar imagem da atualização**.

Na seção **Configuração avançada** da guia **Imagem**, você pode especificar a **Porta do servidor** em que o servidor HTTP escutará bem como o tipo de **Autenticação** usada pelo servidor HTTP. Por padrão, a Porta do servidor é configurada com o valor **2221**. A opção **Autenticação** define o método de autenticação usado para acessar os arquivos de atualização. Estão disponíveis as seguintes opções: **NENHUM, Básico** e **NTLM**. Selecione **Básico** para utilizar a codificação base64, com autenticação básica de nome de usuário e senha. A opção **NTLM** utiliza um método de codificação seguro. Para autenticação, o usuário criado na estação de trabalho que compartilha os arquivos de atualização é utilizado. A configuração padrão é **NENHUM**, que garante acesso aos arquivos de atualização sem necessidade de autenticação.

Aviso:
Se deseja permitir acesso aos arquivos de atualização através do servidor HTTP, a pasta Imagem deve estar localizada no mesmo computador que a instância do ESET NOD32 Antivírus que os criou.

Após concluir a configuração da Imagem, vá até às estações de trabalho e adicione um novo servidor de atualização no formato **http://endereço_IP_do_seu_servidor:2221**. Para fazer isso, siga as etapas a seguir:

- Abra a **Configuração avançada do ESET NOD32 Antivírus** e clique em **Atualizar**.
- Clique em **Editar...** , à direita do menu suspenso **Atualizar servidor** e adicione um novo servidor utilizando o seguinte formato: http://endereço_IP_do_seu_servidor:2221
- Selecione esse servidor recém-adicionado na lista de servidores de atualização.

Acesso à Imagem por meio de compartilhamentos de sistema

Primeiro, uma pasta compartilhada deve ser criada em um local ou em um dispositivo de rede. Ao criar a pasta para a imagem, é necessário fornecer as permissões de "gravação" para o usuário que salvará os arquivos de atualização na pasta e acesso "leitura" para todos os usuários que atualizarão o ESET NOD32 Antivírus na pasta Imagem.

A seguir, configure o acesso à Imagem na seção **Configuração avançada de atualização** (a guia **Imagem**) desativando a opção **Fornecer arquivos de atualização através do servidor HTTP**. Essa opção está ativada por padrão no pacote de instalação do programa.

Se a pasta compartilhada estiver localizada em outro computador na rede, é necessário especificar os dados de autenticação para acessar o outro computador. Para especificar os dados de autenticação, abra a Configuração avançada do ESET NOD32 Antivírus (F5) e clique em **Atualizar**. Clique no botão **Configuração...** e, em seguida, na guia **Rede**. Essa configuração é a mesma para a atualização, conforme descrito no capítulo "Conexão à rede".

Após concluir a configuração da Imagem, prossiga até as estações de trabalho e configure \\UNC\PATH como o servidor de atualização. Essa operação pode ser concluída utilizando as seguintes etapas:

- Abra a Configuração avançada do ESET NOD32 Antivírus (F5) e clique em **Atualizar**.
- Clique em **Editar...** próximo à opção Atualizar servidor e adicione um novo servidor utilizando o formato \\UNC\PATH.
- Selecione esse servidor recém-adicionado na lista de servidores de atualização.

OBSERVAÇÃO: Para o funcionamento adequado, o caminho para a pasta Imagem deve ser especificado como um caminho UNC. A atualização de unidades mapeadas pode não funcionar.

4.2.1.2.4.2 Solução de problemas de atualização da Imagem

Dependendo do método de acesso à pasta Imagem, vários tipos de problemas podem ocorrer. Na maioria dos casos, os problemas que ocorrem durante uma atualização de servidor de Imagem são provocados por ou mais dos seguintes itens: especificação incorreta das opções da pasta Imagem, dados de autenticação incorretos para a pasta Imagem, configuração incorreta nas estações de trabalho locais que tentam fazer download de arquivos de atualização em Imagem ou por uma combinação dessas razões citadas. Aqui é fornecida uma visão geral dos problemas mais freqüentes que podem ocorrer durante uma atualização da Imagem:

- **O ESET NOD32 Antivírus relata um erro ao conectar a um servidor de Imagem** – provavelmente provocado pela especificação incorreta do servidor de atualização (caminho de rede para a pasta Imagem), a partir do qual as estações de trabalho locais fazem download de atualizações. Para verificar a pasta, clique em Windows **menu Iniciar**, clique em **Executar**, insira o nome da pasta e clique em**OK**. O conteúdo da pasta deve ser exibido.
- **O ESET NOD32 Antivírus requer um nome de usuário e uma senha** – provavelmente provocado pela entrada incorreta de dados de autenticação (Nome do usuário e Senha) na seção de atualização. O Nome do usuário e a Senha são utilizados para garantir acesso ao servidor de atualização, a partir do qual o programa se atualizará a si próprio. Verifique se os dados de autenticação estão corretos e inseridos no formato correto. Por exemplo, *Domínio/Nome de usuário* ou *Grupo de trabalho/Nome do usuário*, além das Senhas correspondentes. Se o servidor da Imagem pode ser acessado por "Todos", esteja ciente de que isso não significa que o acesso é garantido a qualquer usuário. "Todos" não significa qualquer usuário não autorizado; apenas significa que a pasta pode ser acessada por todos os usuários do domínio. Como resultado, se a pasta pode ser acessada por "Todos", um nome de usuário e uma senha ainda precisarão ser inseridos na seção de configuração da atualização.
- **O ESET NOD32 Antivírus relata um erro ao conectar a um servidor de imagem** –comunicação na porta definida para acessar a versão HTTP da Imagem está bloqueada.

4.2.2 Como criar tarefas de atualização

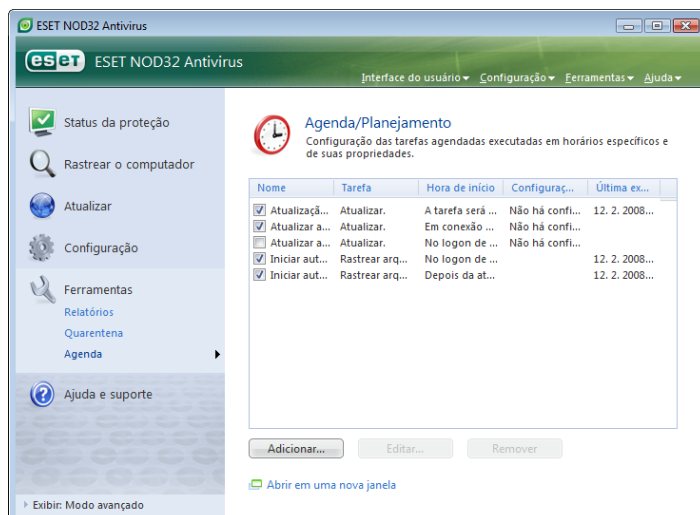
As atualizações podem ser disparadas manualmente clicando em **Atualizar base de dados de assinatura de vírus** na janela de informações exibida após clicar em **Atualizar** no menu principal**.**

As atualizações também podem ser executadas como tarefas agendadas – Para configurar uma tarefa agendada, clique em **Ferramentas > Agenda**. Por padrão, as seguintes tarefas são ativadas no ESET Smart Security:

- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up**
- **Atualizar automaticamente após logon do usuário**

Cada uma das tarefas de atualização mencionadas pode ser modificada para atender às necessidades do usuário. Além das tarefas de atualização padrão, você pode criar novas tarefas de atualização com uma configuração definida pelo usuário. Para obter mais detalhes sobre a criação e a configuração de tarefas de atualização, consulte o capítulo "Agenda".

4.3 Agenda

A Agenda estará disponível se o Modo avançado no ESET NOD32 Antivírus estiver ativado. A **Agenda** pode ser encontrada no menu principal do ESET NOD32 Antivírus em **Ferramentas**. A Agenda contém uma lista resumida de todas as tarefas agendadas e suas propriedades de configuração, como a data e o horário predefinidos e o perfil de rastreamento utilizado.

Por padrão, as seguintes tarefas agendadas são exibidas na **Agenda**:

- **Atualização automática de rotina**
- **Atualizar automaticamente após a conexão dial-up**
- **Atualizar automaticamente após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema após logon do usuário**
- **Rastreamento de arquivos em execução durante inicialização do sistema após atualização bem-sucedida da base de dados de assinatura de vírus**

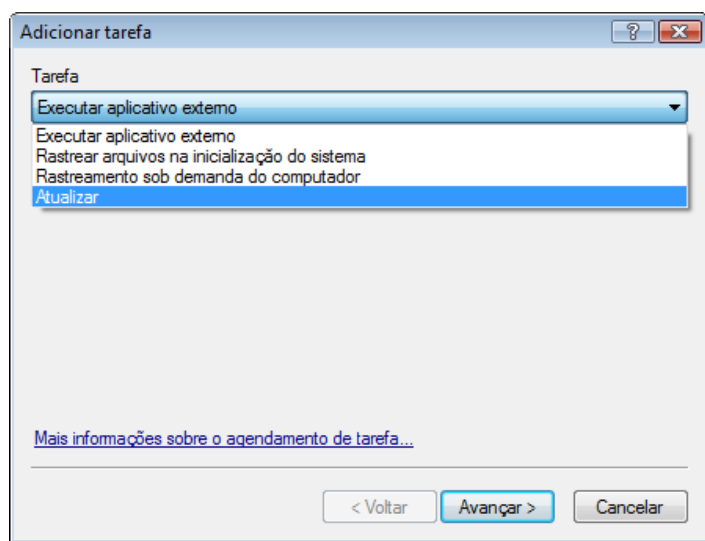
Para editar a configuração de uma tarefa agendada existente (tanto padrão quanto definida pelo usuário), clique com o botão direito do mouse na tarefa e clique em **Editar...** ou selecione a tarefa que deseja modificada e clique no botão **Editar...**

4.3.1 Finalidade do agendamento de tarefas

A Agenda gerencia e inicia tarefas agendadas com as configurações e propriedades predefinidas. A configuração e as propriedades contêm informações, como a data e o horário, bem como os perfis especificados para serem utilizados durante a execução da tarefa.

4.3.2 Criação de novas tarefas

Para criar uma nova tarefa na Agenda, clique no botão **Adicionar...** ou clique com o botão direito do mouse e selecione **Adicionar...** no menu de contexto. Cinco tipos de tarefas agendadas estão disponíveis:

- **Executar aplicativo externo**
- **Manutenção de relatório**
- **Rastrear arquivos na inicialização do sistema**
- **Rastreamento sob demanda do computador**
- **Atualizar**

Como **Rastreamento sob demanda do computador e Atualizar** são as tarefas utilizadas mais freqüentemente, explicaremos como adicionar uma nova tarefa de atualização.

No menu suspenso **Tarefa agendada:**, selecione **Atualizar**. Clique em **Avançar** e insira o nome da tarefa no campo **Nome da tarefa:**. Selecione a freqüência da tarefa. Estão disponíveis as seguintes opções: **Uma vez, Repetidamente, Diariamente**, **Semanalmente** e **Disparado por evento**. Com base na freqüência selecionada, diferentes parâmetros de atualização serão exibidos para você. A seguir, defina que ação tomar se a tarefa não puder ser executada ou concluída na hora agendada. As três opções a seguir estão disponíveis:

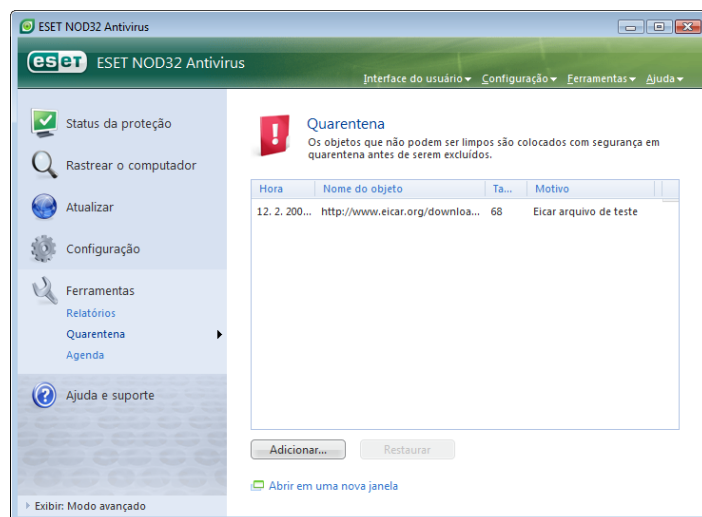
- Aguardar até a próxima hora agendada
- Executar a tarefa tão logo quanto possível
- Executar a tarefa imediatamente se a hora desde a última execução exceder o intervalo especificado (o intervalo pode ser definido imediatamente utilizando a caixa de rolagem Intervalo da tarefa)

Na próxima etapa, uma janela resumida com informações sobre a tarefa agendada atual será exibida; a opção Executar a tarefa com parâmetros específicos deverá ser ativada automaticamente. Clique no botão Finalizar.

Uma janela de diálogo aparecerá permitindo escolher perfis a serem utilizados para a tarefa agendada. Aqui você pode especificar um perfil primário e alternativo, que é utilizando caso a tarefa não possa ser concluída utilizando o perfil primário. Confirme clicando em OK na janela Atualizar perfis. A nova tarefa agendada será adicionada à lista de tarefas agendadas no momento.

4.4 Quarentena

A principal tarefa da quarentena é armazenar com segurança os arquivos infectados. Os arquivos devem ser colocados em quarentena se não puderem ser limpos, se não for seguro nem aconselhável excluí-los ou se eles estiverem sendo falsamente detectados pelo ESET Smart Security.

O usuário pode escolher colocar em quarentena qualquer arquivo que ele ou ela desejar. É aconselhável colocar um arquivo em quarentena se ele se comportar de modo suspeito, mas não for detectado pelo verificador antivírus. Os arquivos colocados em quarentena podem ser enviados aos laboratórios do ESET para análise.

Os arquivos armazenados na pasta de quarentena podem ser visualizados em uma tabela que exibe a data e o horário da quarentena, o caminho para o local original do arquivo infectado, o tamanho do arquivo em bytes, a razão (**adicionado pelo usuário...**) e o número de ameaças (por exemplo, se ele for um arquivo que contém diversas infiltrações).

4.4.1 Arquivos em quarentena

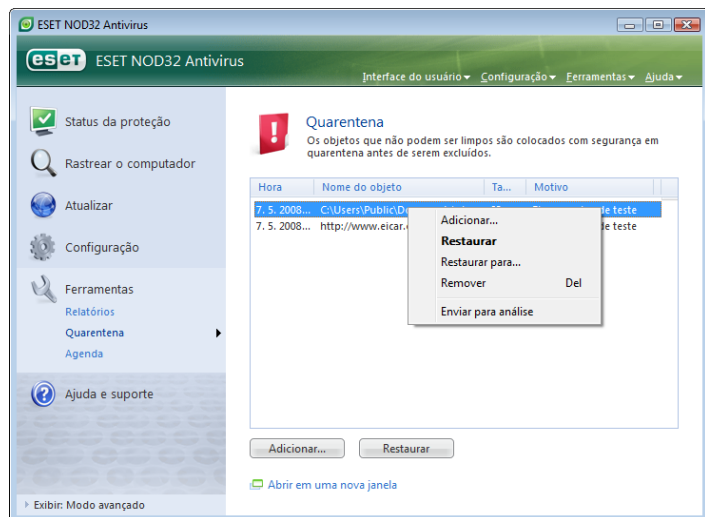
O programa coloca automaticamente os arquivos excluídos em quarentena (se você não cancelou essa opção na janela de alertas). Se desejar, você pode colocar manualmente em quarentena qualquer arquivo suspeito clicando no botão **Adicionar...** Se este for o caso, o arquivo original não será removido do seu local original. O menu de contexto também pode ser utilizado para essa finalidade; clique com o botão direito do mouse na janela de quarentena e selecione **Adicionar...**

4.4.2 Restauração da Quarentena

Os arquivos colocados em quarentena também podem ser restaurados para o local original. Utilize o recurso **Restaurar** para essa finalidade; esse recurso está disponível no menu de contexto clicando com o botão direito do mouse em determinado arquivo, na janela de quarentena. O menu de contexto também oferece a opção **Restaurar para**, que permite que o usuário restaure um arquivo para um local diferente do local original do qual ele foi excluído.

OBSERVAÇÃO:
Se o programa colocou em quarentena um arquivo inofensivo por engano, exclua o arquivo da verificação após restaurá-lo e envie-o para o Atendimento ao cliente da ESET.

4.4.3 Envio de arquivo da Quarentena

Se você colocou em quarentena um arquivo suspeito não detectado pelo programa, ou se um arquivo foi avaliado incorretamente como infectado (por exemplo, pela análise heurística do código) e colocado em quarentena, envie o arquivo para o laboratório da ESET. Para enviar um arquivo diretamente da janela de quarentena, clique com o botão direito do mouse nele e selecione **Enviar para análise** no menu de contexto.

4.5 Relatórios

Os Relatórios contêm as informações sobre todos os eventos importantes do programa que podem ter ocorrido e fornece uma visão geral das ameaças detectadas. As ações de registro em relatórios são uma ferramenta essencial na análise do sistema, detecção de ameaças e solução de problemas. O registro em relatório é realizado ativamente em segundo plano, sem nenhuma interação do usuário. As informações são registradas com base nas configurações do detalhamento do relatório. É possível visualizar mensagens e logs diretamente do ambiente do ESET NOD32 Antivírus, bem como arquivar os registros.

Os relatórios podem ser acessados na janela principal do ESET NOD32 Antivírus clicando em **Ferramentas > Relatórios**. Selecione o tipo de relatório utilizando o menu suspenso **Relatório:** na parte superior da janela. Os seguintes relatórios estão disponíveis:

1. **Ameaças detectadas** – Use esta opção para exibir todas as informações sobre os eventos relacionados à detecção de infiltrações.

2. **Eventos** – Esta opção foi desenvolvida para a solução de problemas de administradores do sistema e usuários. Todas as ações importantes executadas pelo ESET NOD32 Antivírus são registradas nos Relatórios de eventos.

3. **Rastreamento sob demanda do computador** – Os resultados de todos os rastreamentos concluídos são exibidos nessa janela. Clique duas vezes em qualquer entrada para exibir os detalhes do respectivo Rastreamento sob demanda.

Em cada seção, as informações exibidas podem ser copiadas diretamente para a área de transferência, selecionando a entrada e clicando no botão**Copiar**. Para selecionar múltiplas entradas, podem ser usadas as teclas CTRL e SHIFT.

4.5.1 Manutenção dos relatórios

A configuração do Registro em relatórios do ESET NOD32 Antivírus pode ser acessada na janela principal do programa. Clique em **Configuração > Entrar na configuração avançada... > Ferramentas > Relatórios**. Você pode especificar as seguintes opções para os arquivos de relatório:

- **Excluir registros automaticamente:** As entradas de relatório mais antigas que o número de dias especificado são automaticamente excluídas

- **Otimizar automaticamente arquivos de relatório:** Permite a desfragmentação automática dos arquivos de relatório se o percentual especificado de registros inutilizados foi excedido

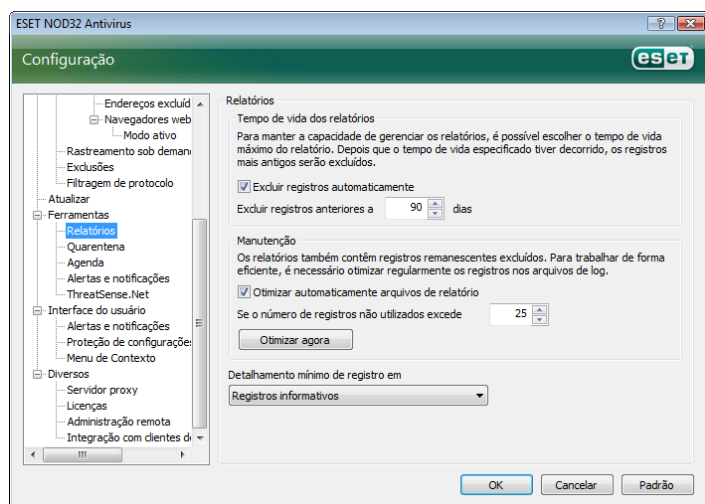
- **Detalhamento mínimo de registro em relatório:** Especifica o nível de detalhamento de registro em relatório. Opções disponíveis:

  - **Erros críticos** – Registra em relatório apenas erros críticos (erro ao iniciar a Proteção antivírus, etc...)

  - **Erros** – Apenas as mensagens “Erro ao fazer download de arquivo” são registradas, além dos erros críticos

  - **Avisos** – Registra mensagens de erros críticos e de avisos

  - **Registros informativos** – Registra as mensagens informativas, incluindo as mensagens de atualização bem-sucedida e todos os registros acima

  - **Registros de diagnóstico** – Registra em relatório informações necessárias para o ajuste otimizado do programa e de todos os registros acima

4.6 Interface do usuário

As opções de configuração da interface do usuário no ESET NOD32 Antivírus podem ser modificadas para que você possa adaptar o ambiente de trabalho conforme suas necessidades. Essas opções de configuração podem ser acessadas em **Interface do usuário** da Configuração avançada do ESET NOD32 Antivírus.

A seção **Elementos da interface do usuário** proporciona aos usuários a capacidade de alternar para Modo avançado. O modo Avançado exibe configurações mais detalhadas e controles adicionais para o ESET Smart Security.

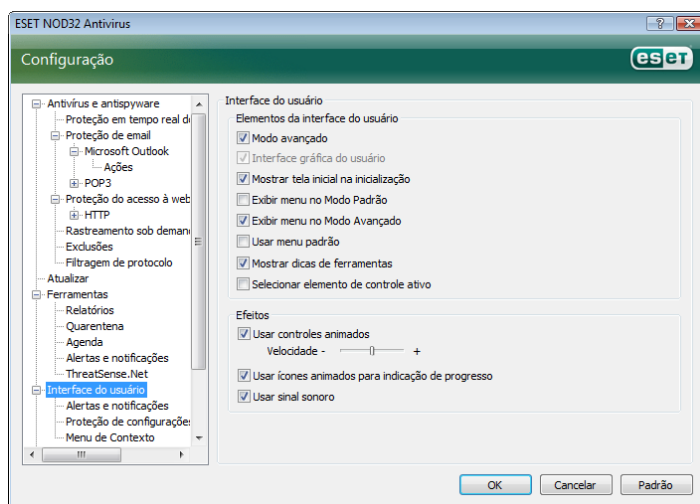
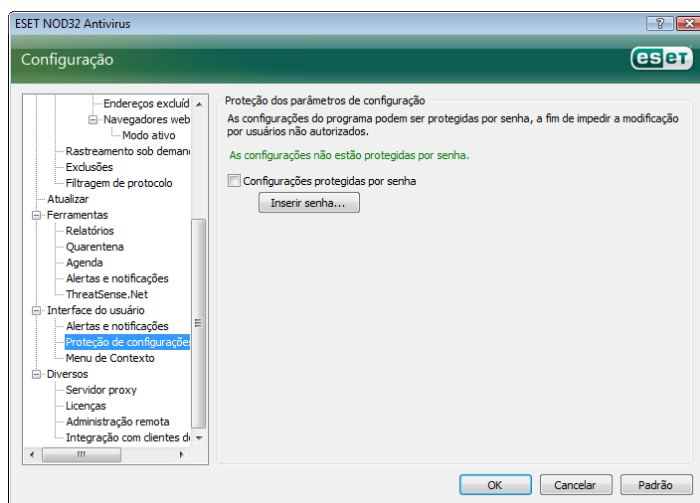
A opção **Interface gráfica do usuário** deve ser desativada se os elementos gráficos reduzirem o desempenho do computador ou provocarem outros problemas. A interface gráfica também pode ser desativada para usuários com deficiência visual, uma vez que pode causar conflito com aplicativos especiais utilizados para leitura do texto exibido na tela.

Se desejar desativar a tela inicial do ESET NOD32 Antivírus, desative a opção **Mostrar tela inicial na inicialização**.

Na parte superior da janela principal do programa ESET NOD32 Antivírus, há um menu Padrão que pode ser ativado ou desativado com base na opção **Usar menu padrão**.

Se a opção **Mostrar dicas de ferramentas** estiver ativada, uma breve descrição de qualquer opção será exibida se o cursor do mouse for colocado sobre a opção desejada. A opção **Selecionar elemento de controle ativo** fará com que o sistema destaque qualquer elemento que esteja atualmente na área ativa do cursor do mouse. O elemento destacado será ativado após um clique do mouse.

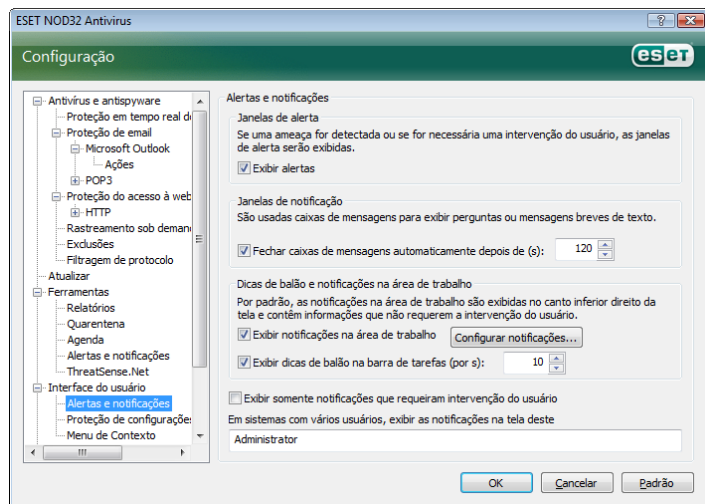
Para reduzir ou aumentar a velocidade dos efeitos animados, selecione a opção **Usar controles animados** e mova o controle deslizante **Velocidade** para a esquerda ou para a direita.

Para ativar o uso de ícones animados a fim de exibir o andamento de diversas operações, marque a caixa de seleção **Usar ícones animados...** Se desejar que o programa emita um aviso sonoro se um evento importante ocorrer, selecione a opção **Usar sinal sonoro**.

Os recursos da **Interface do usuário** também incluem a opção para proteger por senha os parâmetros de configuração do ESET NOD32 Antivírus. Esta opção está localizada no submenu **Proteção de configurações**, em **Interface do usuário**. Para fornecer segurança máxima para o seu sistema, é fundamental que o programa seja configurado corretamente. As modificações não autorizadas podem resultar na perda de dados importantes. Para configurar uma senha para proteger os parâmetros de configuração, clique em **Inserir senha...**

4.6.1 Alertas e notificações

A seção de configuração de **Alertas e notificações** em **Interface do usuário** permite que você configure como as mensagens de alerta de ameaças e as notificações do sistema serão tratadas no ESET Smart Security.

O primeiro item é **Exibir alertas**. A desativação dessa opção cancelará todas as janelas de alerta e é adequada apenas para uma quantidade limitada de situações específicas. Para a maioria dos usuários, recomendamos que esta opção seja mantida como a configuração padrão (ativada).

Para fechar as janelas pop-up automaticamente após um certo período de tempo, selecione a opção **Fechar caixas de mensagens automaticamente depois de (s):**. Se não forem fechadas manualmente pelo usuário, as janelas de alerta serão fechadas automaticamente após o período de tempo especificado ter expirado.

As notificações na área de trabalho e as dicas de balão são apenas informativas e não fornecem nem requerem interação com o usuário. Elas são exibidas na área de notificação, no canto inferior direito da tela. Para ativar a exibição de notificações na área de trabalho, selecione a opção **Exibir notificações na área de trabalho**. Opções mais detalhadas – o tempo de exibição e a transparência da janela de notificação podem ser modificados clicando no botão **Configurar notificações...** Para visualizar o comportamento das notificações, clique no botão **Visualizar**. Para configurar a duração do tempo de exibição das dicas de balão, consulte a opção **Exibir dicas de balão na barra de tarefas (por s):**.

Na seção inferior da janela de configuração **Alertas e notificações**, há a opção **Exibir somente notificações que requeiram intervenção do usuário**. Esta opção permite ativar/desativar a exibição de alertas e notificações que não requeiram intervenção do usuário. O último recurso dessa seção é a especificação de endereços de notificações em um ambiente com vários usuários.

O campo **Em sistemas com vários usuários, exibir as notificações na tela do usuário**: permite que o usuário defina quem receberá notificações importantes do ESET Smart Security. Normalmente, essa pessoa seria um administrador de sistema ou de rede. Esta opção é especialmente útil para servidores de terminal, desde que todas as notificações do sistema sejam enviadas para o administrador.

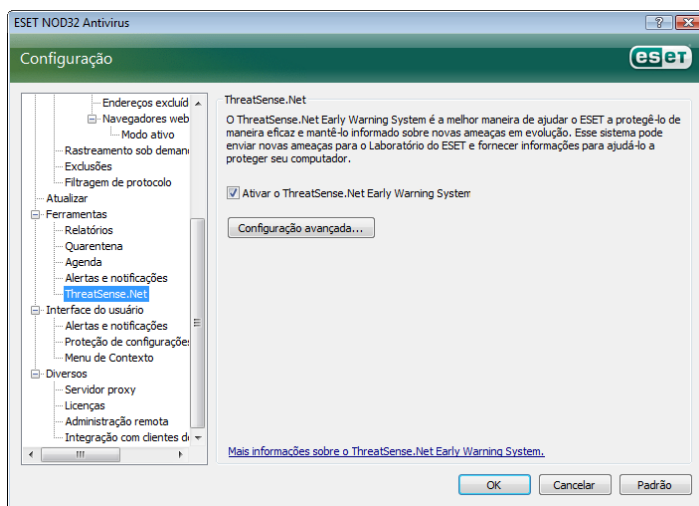
4.7 ThreatSense.Net

O ThreatSense.Net Early Warning System é uma ferramenta que mantém o ESET contínua e imediatamente informado sobr e novas infiltrações. O sistema de alerta bidirecional do ThreatSense.Net tem uma única finalidade: melhorar a proteção que podemos proporcionar-lhe. A melhor maneira de garantir que vemos novas ameaças assim que elas aparecem é fazermos “link” com o máximo possível de nossos clientes e usá-los como nossos Sentinelas de ameaças. Há duas opções:

- Você pode decidir não ativar o ThreatSense.Net Early Warning System. Você não perderá nenhuma funcionalidade no software e receberá a melhor proteção que podemos proporcionar.
- Você pode configurar o sistema de alerta para enviar informações anônimas sobre as novas ameaças e onde o novo código de ameaça está contido em único arquivo. Esse arquivo pode ser enviado para o ESET para análise detalhada. O estudo dessas ameaças ajudará o ESET a atualizar suas capacidades de detecção de ameaças. O ThreatSense.Net Early Warning System coletará informações sobre o seu computador relacionadas a ameaças recém-detectadas. Essas informações podem incluir uma amostra ou cópia do arquivo no qual a ameaça apareceu, o caminho para o arquivo, o nome do arquivo, informações sobre a data e a hora, o processo pelo qual a ameaça apareceu no seu computador e informações sobre o sistema operacional do seu computador. Algumas dessas informações podem incluir informações pessoais sobre o usuário do computador, como nomes de usuário em um caminho de diretório etc. Um exemplo das informações de arquivo enviadas está disponível aqui.

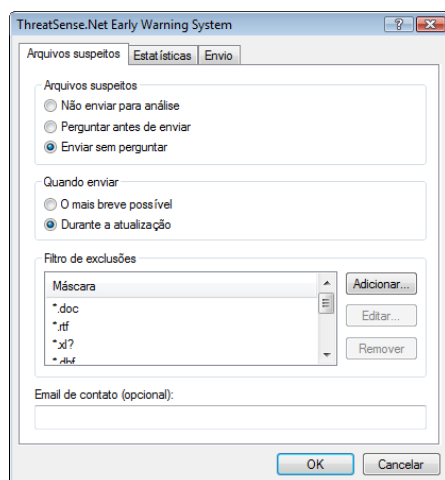
Enquanto há uma possibilidade de que isso possa ocasionalmente revelar algumas informações sobre você ou seu computador para o nosso laboratório de ameaças no ESET, essas informações não serão utilizadas para QUALQUER outra finalidade que não seja nos ajudar a reagir imediatamente contra novas ameaças.

Por padrão, o ESET NOD32 Antivírus é configurado para perguntar antes de enviar arquivos suspeitos ao laboratório de ameaças da ESET para análise detalhada. Deve-se observar que arquivos com certas extensões, como, por exemplo, .doc ou .xls, são sempre excluídos do envio se uma ameaça for detectada neles. Você também pode adicionar outras extensões se houver arquivos específicos que você ou sua empresa desejam impedir o envio.

A configuração do ThreatSense.Net pode ser acessada em Configuração avançada, em **Ferramentas > ThreatSense.Net**. Marque a caixa de seleção **Ativar o ThreatSense.Net Early Warning System** . Essa ação permite que você o ative. Em seguida, clique no botão **Configuração avançada...**

4.7.1 Arquivos suspeitos

A guia **Arquivos suspeitos** permite configurar a maneira em que as ameaças serão enviadas ao laboratório da ESET para análise.

Se você encontrou um arquivo suspeito, você pode enviá-lo ao nosso laboratório de vírus para análise. Se for confirmado que o aplicativo é malicioso, sua detecção será adicionada à próxima atualização de assinatura de vírus.

O envio de arquivos pode ser configurado para ser executado automaticamente sem perguntar. Se esta opção estiver selecionada, os arquivos suspeitos serão enviados no segundo plano. Se desejar saber quais arquivos foram enviados para análise e confirmar o envio, selecione a opção **Perguntar antes de enviar**.

Se não desejar que os arquivos sejam enviados, selecione **Não enviar para análise**. Observe que o não envio de arquivo para análise não afeta o envio de informações estatísticas para o ESET. As informações estatísticas estão configuradas na sua própria seção de configuração, descrita no próximo capítulo.

Quando enviar
Os arquivos suspeitos serão enviados aos laboratórios da ESET para análise o mais breve possível. Esta é a opção recomendada se uma conexão permanente com a Internet estiver disponível e os arquivos suspeitos puderem ser enviados sem atraso. A outra opção é enviar arquivos suspeitos **Durante a atualização**. Se esta opção estiver selecionada, os arquivos suspeitos serão coletados e será feito upload deles para os servidores do Early Warning System durante uma atualização.

Filtro de exclusões
Nem todos os arquivos têm de ser enviados para análise. O Filtro de exclusões permite excluir certos arquivos/pastas do envio. Por exemplo, pode ser útil para excluir arquivos que podem ter informações potencialmente sigilosas, como documentos ou planilhas. Os tipos de arquivos mais comuns são excluídos por padrão (Microsoft Office, OpenOffice). A lista dos arquivos excluídos pode ser ampliada, se desejar.

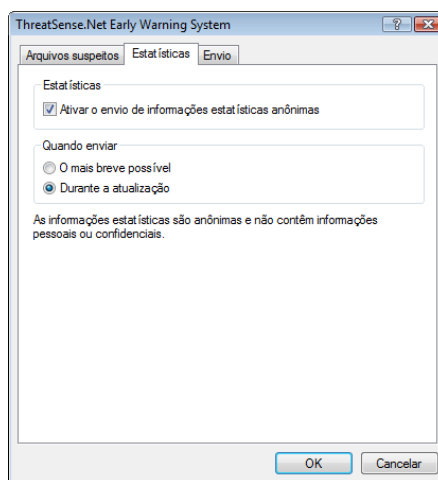
E-mail de contato
O e-mail de contato é enviado à ESET junto com os arquivos suspeitos e pode ser usado para entrar em contato com você se precisarmos de mais informações sobre os arquivos enviados para análise. Observe que você não receberá uma resposta do ESET, a menos que mais informações sejam necessárias.

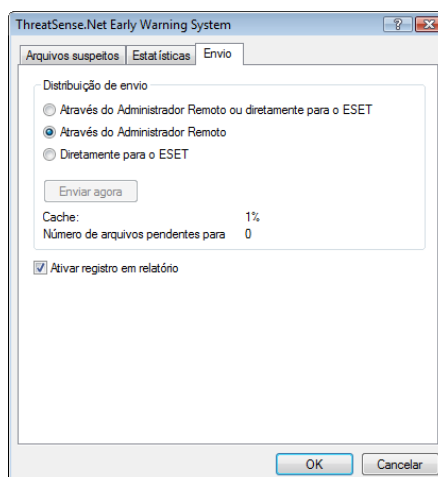
4.7.2 Estatísticas

O ThreatSense.Net Early Warning System coleta informações anônimas sobre o seu computador que sejam relacionadas a ameaças recém-detectadas. Essas informações podem incluir o nome da ameaça, a data e o horário em que ela foi detectada, a versão do ESET NOD32 Antivírus, a versão do sistema operacional do computador e a configuração de local. As estatísticas são normalmente enviadas para os servidores da ESET uma ou duas vezes por dia.

Um exemplo de um pacote estatístico enviado:

```
# utc_time=2005-04-14 07:21:28
# country="Slovakia"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\
Local Settings\Temporary Internet Files\Content.IE5\
C14J8NS7\rdgFR1463[1].exe
```

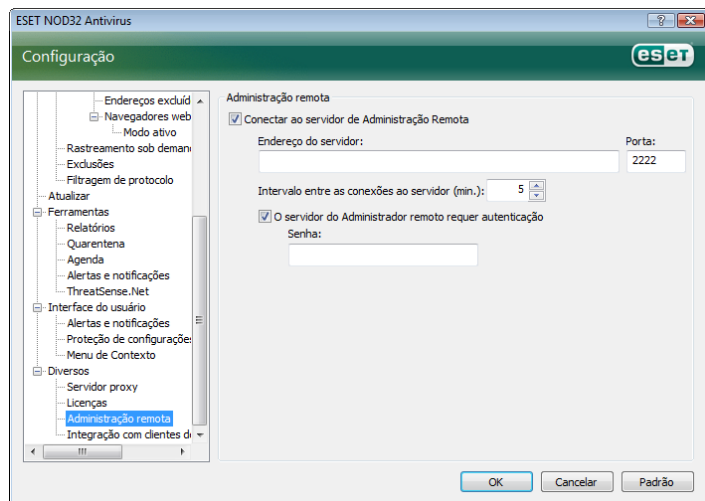
Quando enviar
Na seção **Quando enviar**, é possível definir quando as informações estatísticas serão enviadas. Se escolher enviar **O mais breve possível**, as informações estatísticas serão enviadas imediatamente após serem criadas. Esta configuração é adequada se um conexão permanente com a Internet estiver disponível. Se a opção **Durante a atualização** estiver selecionada, informações estatísticas serão mantidas e enviadas em grupo durante a próxima atualização.

4.7.3 Envio

Nesta seção, você pode escolher se os arquivos e informações estatísticas serão enviados usando o Administrador remoto da ESET ou diretamente para a ESET. Se desejar ter certeza de que os arquivos suspeitos e as informações estatísticas serão enviados para o ESET, selecione a opção **Usando o Administrador remoto ou diretamente para o ESET**. Se esta opção estiver selecionada, os arquivos e estatísticas serão enviados usando todos os meios disponíveis. O envio de arquivos suspeitos usando o Administrador remoto envia arquivos e estatísticas para o servidor do administrador remoto, que garantirá o envio posterior para os laboratórios de vírus da ESET. Se a opção **Diretamente para o ESET** estiver selecionada, todos os arquivos suspeitos e informações estatísticas serão enviados para o laboratório de vírus do ESET diretamente do programa.

Quando houver arquivos com envio pendente, o botão **Enviar agora** estará ativado nessa janela de configuração. Clique neste botão se desejar enviar os arquivos e informações estatísticas imediatamente.

Marque a opção **Ativar registro em relatório** para ativar o registro do envio de arquivos e de informações estatísticas. Após todo envio de um arquivo suspeito ou de uma parte de informações estatísticas, é criada uma entrada no relatório de eventos.

4.8 Administração remota

A Administração remota é uma ferramenta poderosa para a manutenção da política de segurança e para a obtenção de uma visão geral do gerenciamento de segurança dentro da rede. É especialmente útil quando aplicada a redes maiores. A Administração Remota não apenas aumenta o nível de segurança, mas também fornece facilidade de uso na administração do ESET NOD32 Antivírus em estações de trabalho cliente.

As opções de configuração da Administração remota estão disponíveis na janela principal do programa ESET NOD32 Antivírus. Clique em **Configuração > Entrar na configuração avançada... > Diversos > Administração remota**.

A janela Configuração permite ativar o modo de administração remota selecionando primeiro a caixa de seleção **Conectar ao servidor de Administração remota**. É possível acessar as outras opções descritas a seguir:

- **Endereço do servidor** – Endereço de rede do servidor em que o servidor da administração remota está instalado.

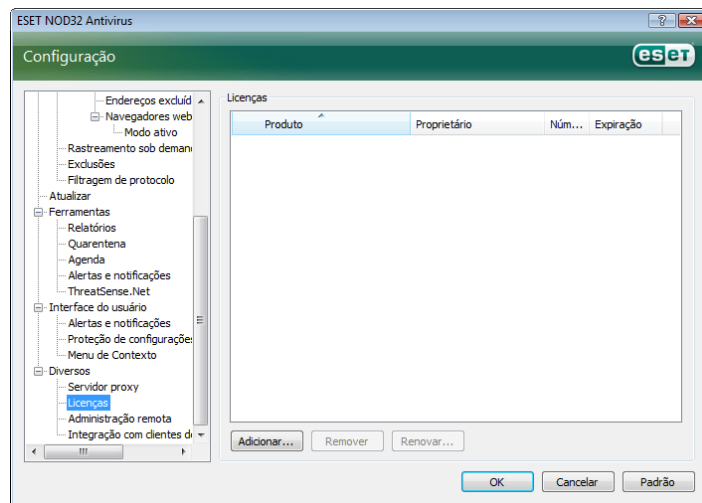
- **Porta** – Este campo contém uma porta de servidor predefinida utilizada para conexão. Recomendamos que você deixe a configuração de porta predefinida em 2222.

- **Intervalo entre as conexões ao servidor (min.)** – Essa opção designa a freqüência em que o ESET NOD32 Antivírus se conectará ao servidor ERA para emitir dados. Em outras palavras, as informações são enviadas nos intervalos de tempo definidos aqui. Se estiver configurado como 0, as informações serão enviadas a cada 5 segundos.

- **O servidor do Administrador remoto requer autenticação** – Permite inserir uma senha para conectar-se ao servidor do administrador remoto, se solicitada.

Clique em **OK** para confirmar as alterações e aplicar as configurações. O ESET NOD32 Antivírus utilizará essas configurações para conectar-se ao servidor remoto.

4.9 Licença

A ramificação **Licença** permite gerenciar as chaves de licença do ESET NOD32 Antivírus e outros produtos da ESET. Após a compra, as chaves de licença são enviadas junto com seu Nome de usuário e Senha. Para **Adicionar/remover** uma chave de licença, clique no botão correspondente na janela do gerenciador de licenças. O gerenciador de licenças pode ser acessado em Configuração avançada, em **Diversos > Licenças**.

A chave de licença é um arquivo de texto que contém informações sobre o produto comprado: o proprietário, o número de licenças e a data de expiração.

A janela do gerenciador de licenças permite que o usuário faça upload e visualize o conteúdo de uma chave de licença utilizando o botão **Adicionar**...; as informações contidas são exibidas no gerenciador. Para excluir os arquivos de licença da lista, clique em **Remover**.

Se uma chave de licença expirou e você estiver interessado em comprar uma renovação, clique no botão **Solicitar...**; você será redirecionado para a nossa loja on-line.

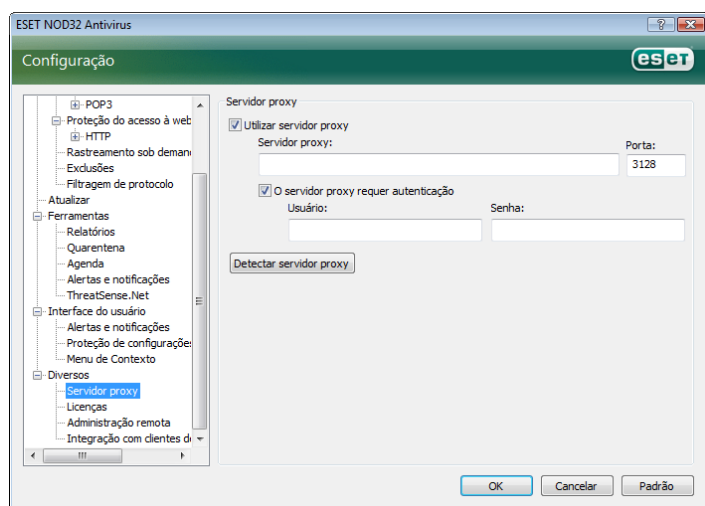
5. Usuário avançado

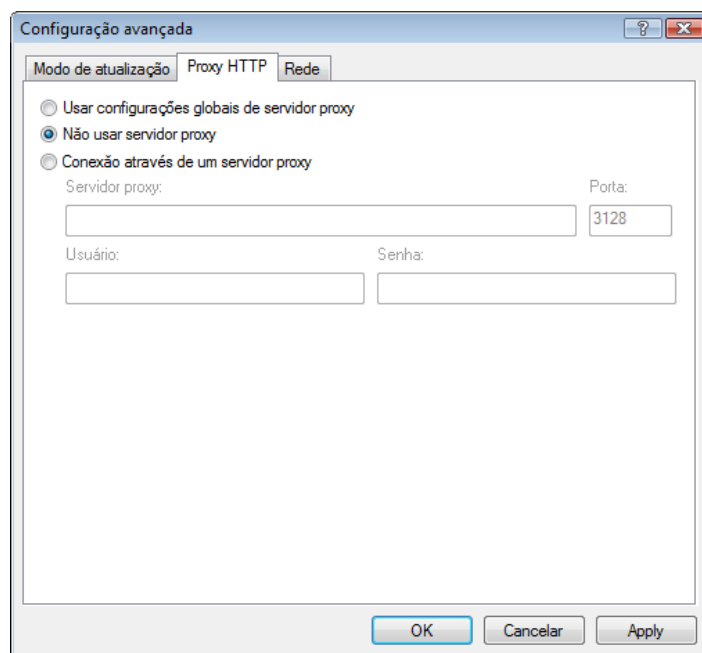
Este capítulo descreve os recursos do ESET NOD32 Antivírus que podem ser úteis para usuários mais avançados. As opções de configuração desses recursos podem ser acessadas somente no Modo avançado. Para alternar para o Modo avançado, clique em **Alternar para modo avançado** no canto inferior esquerdo da janela principal do programa ou pressione CTRL + M no seu teclado.

5.1 Configuração do servidor proxy

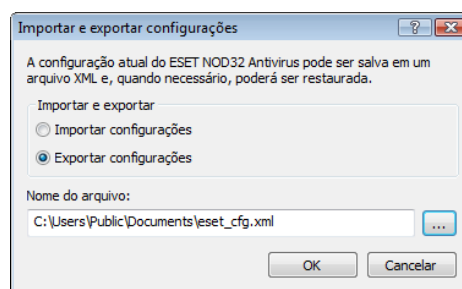
No ESET Smart Security, a configuração do servidor proxy está disponível em duas seções diferentes dentro da estrutura da Configuração avançada.

Primeiro, as configurações do servidor proxy podem ser configuradas em **Diversos > Servidor proxy**. A especificação do servidor proxy neste nível define as configurações globais do servidor proxy para todo o ESET Smart Security. Os parâmetros aqui serão utilizados por todos os módulos que requerem conexão com a Internet.

Para especificar as configurações do servidor proxy para este nível, marque a caixa de seleção **Utilizar servidor proxy** e, em seguida, insira o endereço do servidor proxy no campo **Servidor proxy:**, juntamente com o número da **Porta** do servidor proxy.

Se a comunicação com o servidor proxy requer autenticação, marque a caixa de seleção **O servidor proxy requer autenticação** e insira um **Nome de usuário** e **Senha** válidos nos respectivos campos. Clique no botão **Detectar servidor proxy** para detectar e inserir automaticamente as configurações do servidor proxy. Os parâmetros especificados no Internet Explorer serão copiados. Observe que este recurso não recupera dados de autenticação (Nome de usuário e Senha); eles devem ser fornecidos pelo usuário.

As configurações do servidor proxy podem ser estabelecidas dentro da **Configuração avançada de atualização** (ramificação **Atualizar** da árvore Configuração avançada). Esta configuração é aplicada para o perfl de atualização fornecido e é recomendada para laptops, uma vez que eles freqüentemente recebem atualizações de assinatura de vírus de diferentes locais. Para obter mais informações sobre essa configuração, consulte a Seção 4.4, "Atualização do sistema".

5.2 Exportar/importar configurações

A exportação e a importação da configuração atual do ESET NOD32 Antivírus está disponível no Modo avançado em **Configuração**.

Tanto a exportação como a importação utilizam o tipo de arquivo .xml. A exportação e a importação são úteis se você precisar fazer backup da configuração atual do ESET NOD32 Antivírus para poder utilizá-lo posteriormente (por qualquer razão). A opção Exportar configurações também será útil para aqueles que desejam utilizar a configuração favorita do ESET NOD32 Antivírus em diversos sistemas; eles precisam apenas importar o arquivo .xml.

5.2.1 Exportar configurações

A exportação da configuração é muito fácil. Se desejar salvar a configuração atual do ESET Smart Security, clique em **Configuração > Importar e exportar configurações...** Selecione a opção **Exportar configurações** e insira o nome do arquivo de configuração. Utilize o navegador para selecionar um local no computador no qual deseja salvar o arquivo de configuração.

5.2.2 Importar configurações

As etapas para importar uma configuração são muito semelhantes. Selecione novamente **Importar e exportar configurações** e selecione a opção **Importar configurações**. Clique no botão **...** e procure o arquivo de configuração que deseja importar.

5.3 Linha de comandos

O módulo antivírus do ESET NOD32 Antivírus pode ser iniciado pela linha de comandos: manualmente (com o comando "ecls") ou com um arquivo em lotes ("bat").

Os seguintes parâmetros e chaves podem ser utilizados ao executar o rastreador sob demanda na linha de comandos:

Opções gerais:

– ajuda	mostrar ajuda e sair
– versão	mostrar informações de versão e sair
– base-dir = PASTA	carregar módulos da PASTA
– quar-dir = PASTA	PASTA de quarentena
– aind	mostrar indicador de atividade
– auto	verifica todos os discos rígidos no modo de limpeza

Alvos:

– arquivos	rastrear arquivos (padrão)
– no-files	não rastrear arquivos
– boots	rastrear setores de inicialização (padrão)
– no-boots	não rastrear setores de inicialização
– arch	rastrear arquivos mortos (padrão)
– no-arch	não rastrear arquivos mortos
– max-archive-level = NÍVEL	NÍVEL máximo de encadeamento de arquivos mortos
– scan-timeout = LIMITE	rastrear arquivos mortos pelo LIMITE máximo de segundos. Se o tempo de rastreamento atingir esse limite, o rastreamento do arquivo morto está interrompido, e o rastreamento continuará com o próximo arquivo
– max-arch-size=TAMANHO	verificar somente os primeiros bytes de TAMANHO nos arquivos mortos (padrão 0 = sem limite)
– mail	rastrear arquivos de e-mail
– nomail	não rastrear arquivos de e-mail
– sfx	rastrear arquivos mortos de autoextração
– nosfx	não rastrear arquivos mortos de autoextração
– rtp	rastrear empacotadores em tempo real
– nortp	não rastrear empacotadores em tempo real
– exclude = PASTA	excluir PASTA do rastreamento
– ubdir	rastrear subpastas (padrão)
– nosubdir	não rastrear subpastas
– maxsubdirlevel = NÍVEL	NÍVEL máximo de encadeamento de subpastas (padrão 0 = sem limite)
– symlink	seguir links simbólicos (padrão)
– nosymlink	ignorar links simbólicos
– extremove = EXTENSÕES	
– extexclude = EXTENSÕES	excluir do rastreamento EXTENSÕES delimitadas por dois pontos

Métodos:

– adware	rastrear se há Adware/Spyware/Riskware
– no-adware	não verificar se há Adware/Spyware/Riskware
– unsafe	rastrear por aplicativos potencialmente inseguros
– no-unsafe	não rastrear por aplicativos potencialmente inseguros
– unwanted	rastrear por aplicativos potencialmente indesejados
– no-unwanted	não rastrear por aplicativos potencialmente indesejados
– pattern	usar assinaturas
– no-pattern	não usar assinaturas
– heur	ativar heurística
– no-heur	desativar heurística
– adv-heur	ativar heurística avançada
– no-adv-heur	desativar heurística avançada

Limpeza:

– action = AÇÃO	executar AÇÃO em objetos infectados. Ações disponíveis: nenhum, limpar, aviso
– quarentena	copiar os arquivos infectados para Quarentena (completa AÇÃO)
– noquarantine	não copiar arquivos infectados para Quarentena

Relatórios:

– log-file=ARQUIVO	registrar o relatório em ARQUIVO
– log-rewrite	substituir arquivo de saída (padrão – acrescentar)
– Registrartudo no relatório	também registrar arquivos limpos
– nologall	não registrar arquivos limpos (padrão)

Os possíveis códigos de saída da verificação:

0 – nenhuma ameaça encontrada
1 – ameaça encontrada mas não foi limpa
10 – alguns arquivos infectados não foram limpos
101 – erro no arquivo morto
102 – erro de acesso
103 – erro interno

OBSERVAÇÃO:

Os códigos de saída maiores que 100 significam que o arquivo não foi verificado e, portanto, pode estar infectado.

6. Glossário

6.1 Tipos de infiltrações

A infiltração é uma parte do software malicioso que tenta entrar e/ou danificar o computador do usuário.

6.1.1 Vírus

Um vírus de computador é uma ameaça que corrompe os arquivos existentes em seu computador. O nome vírus vem do nome dos vírus biológicos, uma vez que eles usam técnicas similares para se espalhar de um computador para outro.

Os vírus de computador atacam principalmente os arquivos e documentos executáveis. Para se replicar, um vírus anexa seu "corpo" ao final de um arquivo de destino. Em resumo, é assim que um vírus de computador funciona: após a execução de um arquivo infectado, o vírus ativa a si próprio (antes do aplicativo original) e realiza sua tarefa predefinida. Somente após isso, o aplicativo original pode ser executado. Um vírus não pode infectar um computador a menos que o usuário (acidental ou deliberadamente) execute ou abra ele mesmo o programa malicioso.

Os vírus de computador podem se ampliar em atividade e gravidade. Alguns deles são extremamente perigosos devido à sua capacidade de propositalmente excluir arquivos do disco rígido. Por outro lado, alguns vírus não causam danos reais; eles servem somente para perturbar o usuário e demonstrar as habilidades técnicas dos seus autores.

É importante observar que os vírus estão (quando comparados aos cavalos de tróia e aos spywares) gradualmente se tornando uma raridade, uma vez que eles não são comercialmente atrativos para os autores dos softwares maliciosos. Além disso, o termo "vírus" é muitas vezes incorretamente usado para cobrir todos os tipos de infiltração. No presente, isso está gradualmente sendo substituído e o novo termo "software malicioso", mais preciso, está sendo usado.

Se o seu computador estiver infectado por um vírus, é necessário restaurar os arquivos infectados para o seu estado original, isto é, limpá-los usando um programa antivírus.

Os exemplos de vírus são: OneHalf, Tenga e Yankee Doodle.

6.1.2 Worms

Um worm de computador é um programa contendo código malicioso que ataca os computadores host e se espalha pela rede. A diferença básica entre um vírus e um worm é que os worms têm a capacidade de se replicar e viajam por conta própria. Eles não dependem dos arquivos host (ou dos setores de inicialização).

Os worms se proliferam por e-mail ou por pacotes da rede. Nesse aspecto, os worms podem ser categorizados de dois modos:

- **E-mail**– se distribuem para os endereços de e-mail encontrados na lista de contatos do usuário e
- **Rede** – exploram as vulnerabilidades de segurança dos diversos aplicativos.

Os worms são, portanto, muito mais viáveis do que os vírus de computador. Devido à ampla disponibilidade da Internet, eles podem se espalhar por todo o globo dentro de horas após a sua liberação – em alguns casos, até em minutos. Essa capacidade de se replicar independentemente e de modo rápido os torna mais perigosos do que outros tipos de softwares maliciosos, como os vírus.

Um worm ativado em um sistema pode causar diversas inconveniências: Ele pode excluir arquivos, prejudicar o desempenho do sistema ou até mesmo desativar alguns programas. A natureza de worm de computador qualifica-o como um "meio de transporte" para outros tipos de infiltrações.

Se o seu computador estiver infectado com um worm de computador, recomendamos que exclua os arquivos infectados porque eles provavelmente conterão códigos maliciosos.

Exemplos de worms bem conhecidos são: Lovsan/Blaster, Stration/Warezov, Bagle e Netsky.

6.1.3 Cavalos de Tróia

Historicamente, os cavalos de tróia dos computadores foram definidos como uma classe de infiltração que tenta se apresentar como programas úteis, enganando assim os usuários que os deixam ser executados. Mas é importante observar que isso era verdadeiro para os cavalos de tróia do passado; hoje não há necessidade de eles se disfarçarem. O seu único propósito é se infiltrar o mais facilmente possível e cumprir com seus objetivos maliciosos. O "cavalo de tróia" tornou-se um termo muito genérico para descrever qualquer infiltração que não se encaixe em uma classe específica de infiltração.

Uma vez que essa é uma categoria muito ampla, ela é freqüentemente dividida em muitas subcategorias. As mais amplamente conhecidas são:

- downloader – um programa malicioso com a capacidade de fazer o download de outras infiltrações a partir da Internet.
- dropper – um tipo de cavalo de tróia desenhado para instalar outros tipos de softwares maliciosos em computadores comprometidos.
- backdoor – um aplicativo que se comunica com os agressores remotos, permitindo que eles obtenham acesso ao sistema e assumam o controle dele.
- keylogger – (keystroke logger) – programa que registra cada toque na tecla que o usuário digita e envia as informações para os agressores remotos.
- dialer – dialers são programas desenhados para se conectar aos números premium-rate. É quase impossível para um usuário notar que uma nova conexão foi criada. Os dialers somente podem causar danos aos usuários com modems discados que não são mais usados regularmente.

Os cavalos de tróia geralmente tomam a forma de arquivos executáveis com extensão .exe. Se um arquivo em seu computador for detectado como um cavalo de tróia, é aconselhável excluí-lo, uma vez que ele quase sempre contém códigos maliciosos.

Os exemplos dos cavalos de tróia bem conhecidos são: NetBus, Trojandownloader.Small.ZL, Slapper.

6.1.4 Rootkits

Os rootkits são programas maliciosos que concedem aos agressores da Internet acesso ao sistema, ao mesmo tempo em que ocultam a sua presença. Os rootkits, após acessar um sistema (geralmente explorando uma vulnerabilidade do sistema) usam as funções do sistema operacional para evitar serem detectados pelo software antivírus: eles ocultam processos, arquivos e dados do registro do Windows. Por essa razão, é quase impossível detectá-los usando as técnicas comuns.

Quando se trata de prevenção do rootkit, lembre-se de que há dois níveis de detecção:

1. Quando eles tentam acessar um sistema. Eles ainda não estão presentes e estão, portanto, inativos. A maioria dos sistemas antivírus são capazes de eliminar rootkits nesse nível (presumindo-se que eles realmente detectem tais arquivos como estando infectados).

2. Quando eles estão ocultos para os testes usuais. Os usuários do sistema antivírus ESET têm a vantagem da tecnologia Anti-Stealth, que também é capaz de detectar e eliminar os rootkits ativos.

6.1.5 Adware

Adware é abreviação para advertising-supported software (software suportado por propaganda). Os programas exibindo material de publicidade pertencem a essa categoria. Os aplicativos Adware freqüentemente abrirão automaticamente novas janelas pop-up contendo publicidade no navegador da Internet ou mudarão a homepage deste. O Adware é freqüentemente vinculado a programas freeware, permitindo que os criadores de freeware cubram os custos de desenvolvimento de seus aplicativos (geralmente úteis).

O Adware por si só não é perigoso; os usuários somente serão incomodados pela publicidade. O perigo está no fato de que o adware pode também realizar funções de rastreamento (assim como o spyware faz).

Se você decidir usar um produto freeware, preste especial atenção ao programa da instalação. É muito provável que o instalador notifique você sobre a instalação de um programa adware extra. Normalmente você poderá cancelá-lo e instalar o programa sem o adware. Por outro lado, alguns programas não serão instalados sem o adware ou as suas funcionalidades serão limitadas. Isso significa que o adware poderá acessar com freqüência o sistema de modo "legal" , porque os usuários concordaram com isso. Nesse caso, é melhor prevenir do que remediar.

Se um arquivo for detectado como adware em seu computador, é aconselhável excluí-lo, uma vez que há uma grande probabilidade de ele conter códigos maliciosos.

6.1.6 Spyware

Essa categoria cobre todos os aplicativos que enviam informações privadas sem o consentimento/conhecimento do usuário. Eles usam as funções de rastreamento para enviar diversos dados estatísticos como listas dos websites visitados, endereços de e-mail da lista de contato do usuário ou uma lista das teclas digitadas.

Os autores do spyware alegam que essas técnicas têm por objetivo saber mais sobre as necessidades e interesses dos usuários e permitir publicidade melhor direcionada. O problema é que não há uma distinção clara entre os aplicativos maliciosos e os úteis, e ninguém pode assegurar que as informações recebidas não serão usadas de modo indevido. Os dados obtidos pelos aplicativos spyware podem conter códigos de segurança, PINS, números de contas bancárias, etc. O Spyware freqüentemente é vinculado a versões gratuitas de um programa pelo seu autor a fim de gerar lucro ou para oferecer um incentivo à compra do software. Freqüentemente, os usuários são informados sobre a presença do spyware durante a instalação do programa a fim de fornecer a eles um incentivo para atualizar para uma versão paga sem ele.

Os exemplos de produtos freeware bem conhecidos que vêm vinculados a spyware são os aplicativos clientes das redes P2P (peer-to-peer). O Spyfalcon ou Spy Sheriff (e muitos mais) pertencem a uma subcategoria de spyware específica – eles parecem ser programas antispyware, mas são na verdade spyware eles mesmos.

Se um arquivo for detectado como spyware em seu computador, é aconselhável exclui-lo, uma vez que há uma grande possibilidade de ele conter códigos maliciosos.

6.1.7 Aplicativos potencialmente inseguros

Há muitos programas legítimos que servem para simplificar a administração dos computadores conectados em rede. Entretanto, se em mãos erradas, eles podem ser usados indevidamente para fins maliciosos. Essa é a razão pela qual a ESET criou esta categoria especial. Nossos clientes agora têm a opção de escolher se o sistema antivírus deve ou não detectar tais ameaças.

"Aplicativos potencialmente inseguros" é a classificação usada para softwares comerciais, legítimos. Essa classificação inclui os programas como as ferramentas de acesso remoto, aplicativos para quebra de senha e keyloggers (um programa que grava cada toque nas teclas digitadas pelo usuário).

Se você achar que há um aplicativo não seguro em potencial presente e sendo executado em seu computador (e que você não instalou), favor consultar o seu administrador de rede ou remover o aplicativo.

6.1.8 Aplicativos potencialmente indesejados

Os aplicativos potencialmente indesejados não são necessariamente maliciosos, mas podem afetar o desempenho do seu computador de um modo negativo. Tais aplicativos geralmente exigem o consentimento para a instalação. Se eles estiverem presentes em seu computador, o seu sistema se comportará de modo diferente (em comparação ao estado anterior a sua instalação). As alterações mais significativas são:

- são abertas novas janelas que você não via anteriormente
- ativação e execução de processos ocultos
- uso aumentado de recursos do sistema
- alterações nos resultados de pesquisa
- o aplicativo se comunica com servidores remotos